TP-LINK®

多 WAN 口高性能网吧路由器

TL-ER5120

用户手册

Rev1.2.0
1910040147

声明

本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知。可随时查阅我们的万维网页http://www.tp-link.com.cn。除非有特殊约定，本手册仅作为使用指导，本手册中的所有陈述、信息等均不构成任何形式的担保。

目录

物品清单

请仔细检查包装盒，里面应有以下配件：

- 一台 TP-LINK 多 WAN 口高性能网吧路由器
- 一根 Console 连接线
- 一根电源线
- 一本安装手册
- 一张保修卡
- 一张光盘
- 两个 L 型支架及其他配件

注意：

如果发现有配件短缺或损坏的情况，请及时与当地经销商联系。

第1章 用户手册简介

本手册旨在帮助您正确使用本款路由器。内容包含对路由器性能特征的描述以及配置路由器的详细说明。请在操作前仔细阅读本手册。

1.1 目标读者

本手册的目标读者为熟悉网络基础知识、了解网络术语的技术人员。

1.2 本书约定

在本手册中，

➢ 所提到的“路由器”、“本产品”等名词，如无特别说明，系指 TL-ER5120 多 WAN 口高性能网吧路由器，下面简称为 TL-ER5120。

➢ 用 **>>** 符号表示配置界面的进入顺序。默认为**一级菜单 >> 二级菜单 >> 标签页**，其中，部分功能无二级菜单。

➢ 正文中出现的<>尖括号标记文字，表示 Web 界面的按钮名称，如<确定>。

➢ 正文中出现的“”双引号标记文字，表示 Web 界面出现的除按钮外名词，如“ARP 绑定”界面。

本手册中使用的特殊图标说明如下：

图标	含义
注意：	该图标提醒您对设备的某些功能设置引起注意，如果设置错误可能导致数据丢失，设备损坏等不良后果。
说明：	该图标表示此部分内容是对相应设置、步骤的补充说明。

1.3 章节安排

第 1 章：用户手册简介。帮助快速掌握本手册的结构、了解本手册的约定，从而更有效地使用本手册。

第 2 章：产品介绍。介绍本产品特性、应用以及外观。

第 3 章：配置指南。指导如何登录 TL-ER5120 的 Web 管理界面，并简要介绍界面特点。

第 4 章：功能设置。介绍 TL-ER5120 的所有功能，帮助您更充分地使用本产品。

第 5 章：典型配置。以真实的网吧应用为例，解决实际需求。

第 6 章：命令行简介。介绍路由器 Console 口登录方法及配置中常用的 CLI 命令。

附录 A：常见问题。

附录 B：术语表。

附录 C：规格参数。

第2章 产品介绍

2.1 产品描述

TL-ER5120 是一款多 WAN 口高性能网吧路由器，是 TP-LINK 公司专门为网吧、小区、酒店等提供高速稳定宽带接入而设计的路由器，具有高性能、高稳定、高安全、高灵活四大特点。

TL-ER5120 采用专业的 64 位网络处理器，主频达 500MHz，结合容量为 128MB 的 DDRII-533 高速内存，保证 TL-ER5120 具有高性能数据转发能力。在实际网吧环境中，典型带机量为 250-350 台。

TL-ER5120 采用创新导热式自然散热，无风扇静音设计，内置高品质开关电源，外部采用 1U 钢壳，19 英寸标准机架设计，充分保证整机长时间稳定可靠运行。

TL-ER5120 具有强大的攻击防护功能，不仅能够防御来自局域网的病毒攻击、ARP 攻击和欺骗，还能够防御来自广域网的 ARP 病毒、DoS 等攻击，防止黑客的恶意攻击，保证网吧网络长时间稳定安全运行。

防局域网攻击：

TL-ER5120 支持对局域网内主机的 IP/MAC 信息绑定功能，能有效防范局域网内的 ARP 攻击；同时支持免费 ARP 包定时发送机制，有效避免局域网内的 ARP 欺骗，杜绝局域网内的 ARP 病毒攻击。TL-ER5120 内置高级防火墙和过滤规则，不仅支持基于 IP、MAC、URL 的过滤规则，用户也可以根据协议、端口号来自定义病毒类型，对数据包进行双向检测和过滤，防止 Nimda、冲击波、木马等病毒攻击，为网吧提供可靠的局域网安全保障。

防广域网攻击：

TL-ER5120 支持对连接 WAN 口网关的 IP 与 MAC 信息绑定功能，可防范来自广域网的 ARP 攻击；并提供扫描类、DoS 类、可疑包类等丰富的攻击防护，能侦测及阻挡 IP 地址欺骗、源路由攻击、IP/端口扫描、DoS 等来自广域网的网络攻击。多种广域网防攻击功能全面保障网吧网络安全。

灵活的带宽管理：

TL-ER5120 支持基于 IP 的带宽管理功能，提供“普通带宽控制”和“弹性带宽控制”两种策略，灵活管控网络带宽；支持游戏优先策略，可分配给游戏独立的带宽，保证游戏的畅通；支持连接数限制功能，防止 BT、迅雷等 P2P 软件过度占用带宽。

灵活的设备配置管理：

TL-ER5120 支持配置文件导入导出，配置简单，大大缩短配置时间，保证网吧正常运行；同时采用全中文 Web 管理界面，支持远程管理，支持多种系统检测工具和丰富的日志功能，设备管理维护灵活；支持 WAN 口、LAN 口和 DMZ 口的 MAC 地址修改，网络组建、设备升级更新灵活方便。

灵活的功能设置：

TL-ER5120 支持一对一 NAT 功能，轻松实现分配给特定服务器广域网 IP 地址，避免使用复杂的虚拟服务器规则。支持 ARP 扫描和导入功能，轻松实现全网 ARP 绑定。

2.2 产品特性

硬件特性

- 采用 64 位网络专用处理器，主频 500MHz；
- 配备容量为 128MB 的 DDRII-533 高速内存；
- 提供 5 个 10/100M 自适应以太网接口；
- 提供 1 个硬件 DMZ 接口；
- 提供 1 个 Console 口；
- 内置高品质开关电源，无风扇静音设计；
- 1U 钢壳，可安装于 19 英寸标准机架，工业级设计。

支持协议

- 符合 IEEE 802.3、IEEE 802.3u 标准；
- 支持 TCP/IP，DHCP，ICMP，NAT，NAPT 等协议；
- 支持 PPPoE，SNTP，HTTP，DDNS、UPnP，NTP 等协议。

基本功能

- 支持静态 IP、动态 IP、PPPoE、L2TP 多种接入方式；
- 支持虚拟服务器、端口触发、ALG、静态路由、RIP 动态路由等功能；
- 内置简单管理交换机，支持 VLAN 设置和端口监控等交换机功能；
- 支持 LAN 口、WAN 口以及 DMZ 口的 MAC 地址修改；
- 支持配置文件备份与导入；
- 支持系统日志、日志服务器、流量统计、系统时间设置等功能；
- 支持 Web 和远程管理，全中文配置界面；
- 提供诊断工具（Ping、Tracert），支持 WAN 口在线检测功能。

带宽管理

- 支持基于 IP 的带宽控制，可限制单机带宽；
- 支持连接数设置，可限制单机连接数；
- 提供游戏加速功能，保障游戏小包数据的带宽。

网络安全

- 内建防火墙，支持 URL、MAC 地址过滤；
- 支持访问控制，可自定义服务类型；
- 支持攻击防护功能，可对网络攻击和病毒攻击进行防范；
- 支持局域网 IP/MAC 地址绑定，防范局域网 ARP 攻击；
- 支持广域网 IP/MAC 地址绑定，防范广域网 ARP 攻击；
- 支持定时发送 GARP 包功能，防范局域网 ARP 欺骗。

2.3 产品外观

2.3.1 前面板

TL-ER5120 的前面板由 5 个 10/100M接口、1 个Console接口、指示灯和Reset键组成。如图 2-1所示。

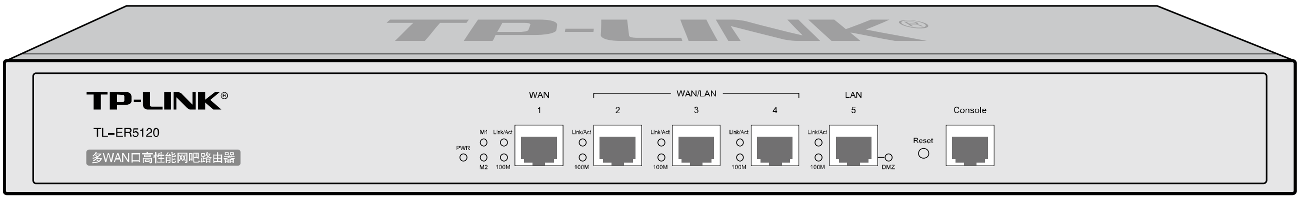


图 2-1 TL-ER5120 前面板示意图

- **5 个 10/100Mbps 自适应 RJ45 接口**

TL-ER5120 支持 10Mbps/100Mbps 带宽的连接设备。每个接口对应一组指示灯，即 Link/Act 和 100M 指示灯。

- **1 个 Console 接口**

Console接口位于面板最右边，使用此接口可以对路由器进行命令行配置，详见**第 6 章命令行简介**。

- **Reset 键**

如果需要将路由器恢复到出厂默认设置，请在路由器通电的情况下，使用尖状物按住路由器前面板的 Reset 键，等待 3-5 秒后，见到 M1 长亮 2-5 秒，松开按键，待 M1 和 M2 两灯同时快闪约 1 秒，此时路由器已成功恢复出厂配置。路由器出厂默认管理地址是 192.168.1.1，默认用户名/密码是 admin/admin。

- **指示灯**

指示灯包括电源 PWR 指示灯，系统状态 M1/M2 指示灯，连接状态 Link/Act 指示灯，100M 速率指示灯，DMZ 接口状态指示灯。通过指示灯可以监控路由器的工作状态，下表将详细说明指示灯工作状态：

指示灯	名称	状态描述
PWR	电源指示灯	常亮表示系统供电正常
		常灭表示电源关闭或电源故障
M1	系统状态指示灯	按下 Reset 键时常亮表示正在恢复出厂配置，与 M2 同时快闪约 1 秒表示恢复出厂配置成功
		系统正常工作时常灭，其他状态表示系统异常
M2	系统状态指示灯	系统正常工作时闪烁（1 次/秒），其他状态表示系统异常
Link/Act	广域网和局域网状态指示灯	常亮表示相应端口已正常连接
		闪烁表示相应端口正在传输数据
		常灭表示相应端口未建立连接
100M	速率指示灯	常亮表示端口速率为 100Mbps
		常灭表示端口速率为 10Mbps 或者未接入设备
DMZ	DMZ 接口状态指示灯	常亮表示 DMZ 接口已启用
		常灭表示 DMZ 接口已关闭

2.3.2 后面板

路由器后面板由电源接口和防雷接地柱组成，如图 2-2所示：

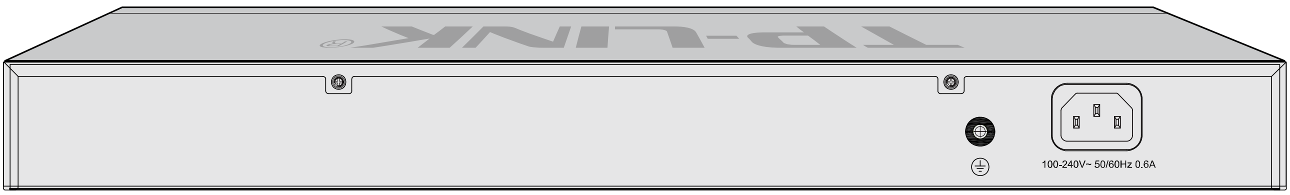


图 2-2 后面板示意图

➢ **电源接口**

位于后面板右侧，接入电源需为 100-240V~ 50/60Hz 0.6A 的交流电源。

➢ **防雷接地柱**

请使用黄绿双色外皮的铜芯导线接地，以防雷击，具体请参考《设备防雷安装手册》。

注意：

- 请使用原装电源线。
- 电源插座请安装在设备附近便于触及的位置，以方便操作。

第3章 配置指南

3.1 登录Web界面

第一次登录时，需要确认以下几点：

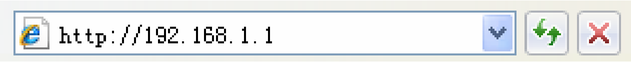
1) 路由器已正常加电启动，任一 LAN 口已与管理主机相连。

2) 管理主机已正确安装有线网卡及该网卡的驱动程序、并已正确安装 IE 6.0 或以上版本的浏览器。

3) 管理主机 IP 地址已设为与路由器 LAN 口同一网段，即 192.168.1.X（X 为 2 至 254 之间的任意整数），子网掩码为 255.255.255.0，默认网关为路由器管理地址 192.168.1.1。也可选择“自动获得 IP 地址”来通过路由器 DHCP 自动分配 IP 地址。

4) 为保证能更好地体验 Web 界面显示效果，建议将显示器的分辨率调整到 1024×768 或以上像素。

打开IE浏览器，在地址栏输入http://192.168.1.1登录TL-ER5120 的Web管理界面。



路由器登录界面如图 3-1所示。



图 3-1 路由器登录界面

在此界面输入路由器管理帐号的用户名和密码，出厂缺省值为admin/admin。成功登录后将看到路由器的系统状态信息，如图 3-2。



图 3-2 TL-ER5120 系统状态

3.2 Web界面简介

3.2.1 界面总览

TL-ER5120 路由器典型的Web界面如图 3-3所示。



图 3-3 典型 Web 界面

在图 3-4 Web界面区域划分中可以看到，左侧为一级、二级菜单栏，右侧上方长条区域为菜单下的标签页，当一个菜单包含多个标签页时，可以通过点击标签页的标题在同级菜单下切换标签页。右侧标签页下方区域可分为两部分，条目配置区以及列表管理区。



图 3-4 Web 界面区域划分

3.2.2 界面常见按钮及操作

➢ 条目配置区常见按钮

按钮	含义
保存	保存当前配置信息。
新增	新增当前配置信息。
修改	修改并保存编辑后的配置信息。
清除	快速清除当前配置项中已输入的所有信息。
帮助	打开当前功能的帮助界面。

说明：

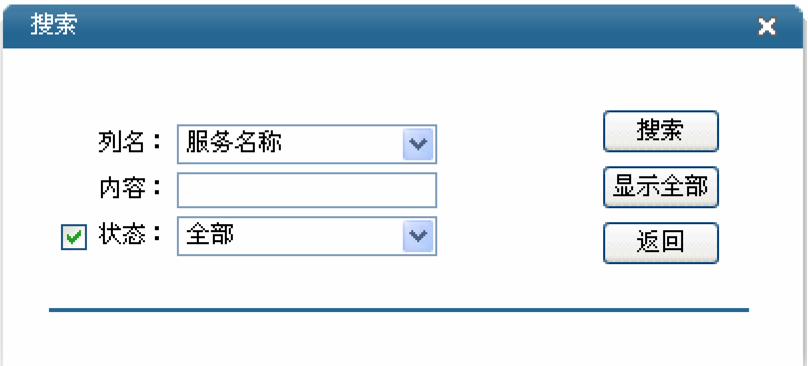
<修改>按钮只有当编辑列表中的规则/条目时才会出现，取代原本的<新增>按钮。

➢ 列表管理区常见按钮

按钮	含义
全选	选中当前列表中所有规则/条目。
启用	启用选中的规则/条目，可批量操作。
禁用	禁用选中的规则/条目，可批量操作。
生效	使选中的规则/条目生效，可批量操作。
不生效	使选中的规则/条目不生效，可批量操作。
删除	删除选中的规则/条目，可批量操作。
刷新	刷新列表。

➢ 列表管理区扩展按钮

搜索　　按照指定关键字段搜索相应的规则。



列名	选择当前列表中任一表头字段。
内容	输入关键字。
状态	指定搜索范围为“启用”、“禁用”或者任意状态下的规则/条目。

➢ 列表管理区常见操作

按钮	名称	含义
	编辑	点击后，需要编辑的规则/条目内容会出现在列表上方的配置管理区，原<新增>按钮同时变为<修改>按钮。在配置管理区修改当前配置后，点击<修改>按钮保存生效。该操作不可批量进行。
	启用/生效	点击后，修改当前规则/条目状态。该操作不可批量进行。
	禁用/不生效	点击后，修改当前规则/条目状态。该操作不可批量进行。
	删除	点击后，删除当前规则/条目。该操作不可批量进行。

第4章 功能设置

4.1 系统维护

系统维护提供路由器系统的最新信息，方便网络管理、故障分析等操作。

4.1.1 系统状态

系统状态界面显示路由器当前硬件和软件版本信息、各接口配置信息以及系统资源使用情况。

界面进入方法：系统维护 >> 系统状态



图 4-1 系统状态界面

4.1.2 接口流量

接口流量界面显示路由器所有正在工作的接口的数据接收/发送速率，以及 WAN 口的附加信息统计。

界面进入方法：系统维护 >> 接口流量

接口流量统计

接口	接收速率 (Kbps)	发送速率 (Kbps)	接收总包数 (Pkt)	发送总包数 (Pkt)	接收总字节数 (Byte)	发送总字节数 (Byte)
WAN1	100	50	1000000000	500000000	1000000000	500000000
WAN2	100	50	100000	50000	100000	50000
LAN	22.2	22.15	22200	22150	100000	50000
DMZ	20.48	20.35	20480	20350	100000	50000

WAN口附加信息

接口	接收IP分片 (Pkt)	接收IP异常包 (Pkt)
WAN1	1	2
WAN2	3	4

刷新 清空统计 帮助

图 4-2 接口流量界面

接收/发送速率是以千比特每秒为单位进行统计的，通常所说的 1M 带宽即 1024Kbps。接收/发送总包数统计的是数据包的总个数。接收/发送总字节数统计的则是所有数据包的总字节数。

WAN 口附加信息则是以数据包为单位进行统计。其中，IP 分片是指接收到的大小超过 WAN 口允许接收的最大值，需要分片传输的数据包；IP 异常包是指 IP 封装字段非正常的数据包。

4.1.3 日志

可以在日志界面查看路由器系统事件的记录信息。

界面进入方法：系统维护 >> 日志

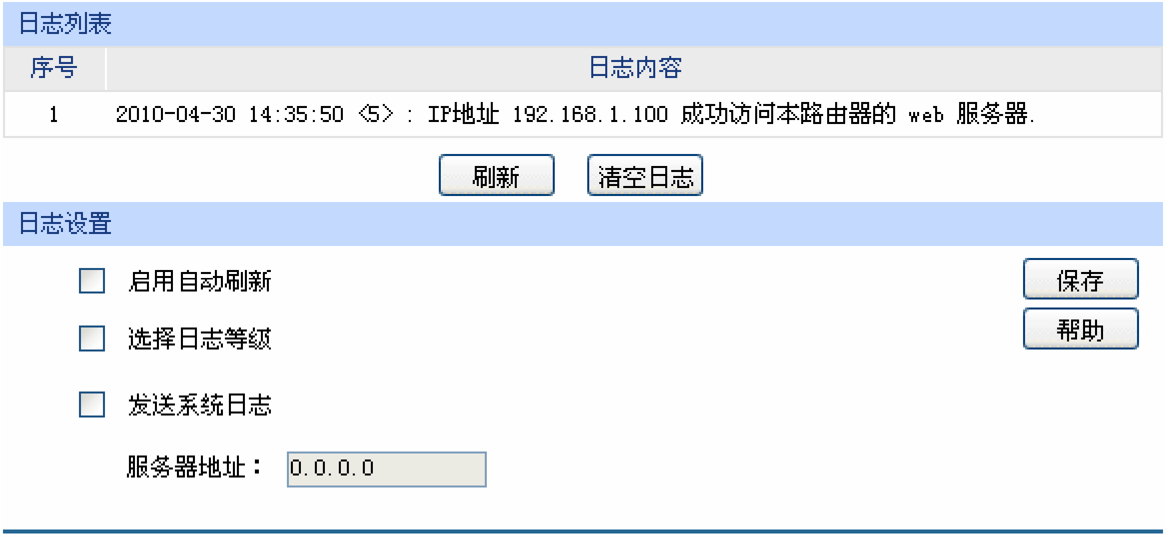
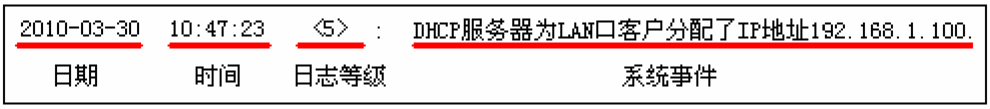
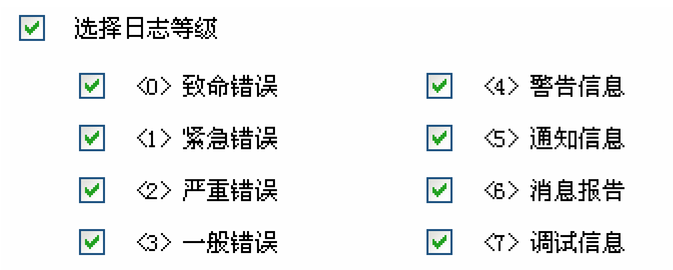


图 4-3 日志界面

日志列表中一条日志内容可分为四个部分：



日志配置部分可以对日志系统进行简单的配置。启用自动刷新后，日志列表将每隔 5 秒刷新一次；选择日志等级可使日志列表中仅列出指定等级的日志记录。



各等级描述：

<0> 致命错误 导致系统不可用的错误，红色显示。

<1> 紧急错误 必须对其采取紧急措施的错误，红色显示。

<2> 严重错误 导致系统处于危险状态的错误，红色显示。

<3> 一般错误 一般性的错误提示，橙色显示。

<4> 警告信息 系统仍然正常运行，但可能存在隐患的提示信息，橙色显示。

<5> 通知信息 正常状态下的重要提示信息。

<6> 消息报告 一般性的提示信息。

<7> 调试信息 调试过程产生的信息。

若需要在某台主机上查看路由器日志信息，请首先在这台主机上安装日志服务器，然后勾选路由器日志页面上的“发送系统日志”选项，并输入这台主机的 IP 地址。保存设置后路由器将向指定地址发送系统日志。

4.1.4　时间设置

时间设置界面允许对路由器的系统时间进行设置。若时间设置发生改变，将会影响一些与其相关的功能，如防火墙规则的生效时间、PPPoE 定时拨号、日志等。

界面进入方法：系统维护 >> 时间设置



图 4-4 时间设置界面

界面项说明：

➢ 当前时间

此处将显示目前系统时间及时间获取方式信息。如果想对时间进行更改，可以在下方时间设置区进行改动。

➢ 时间设置

通过网络获取系统时间　　若路由器可以访问互联网，可以选择此项进行网络校时。选择时区后点击<保存>按钮，路由器将会在内置 NTP(Network Time Protocol, 网络校时协议)服务器地址列表中搜索可用地址，并获取时间。若获取失败，请手动设置 NTP 服务器地址，由于 NTP 服务器并非固定不变，推荐在互联网上搜索两个不同的地址，分别填入首选、备用 NTP 服务器输入

框中，设置完毕后点击<保存>按钮，路由器会通过指定的 NTP 服务器获取网络时间。

手工设置系统时间	若路由器暂时不能访问互联网，可以选择对系统时间进行手动设置，或者点击<获取管理主机时间>按钮，系统将自动填入当前管理主机时间信息。最后请注意点击<保存>生效。

说明

- 如果不能正常使用<获取管理主机时间>功能，需要在主机的防火墙软件中增加 UDP 端口为 123 的例外。
- 断电重启后，断电之前设置的时间将失效，重新变为“通过网络获取时间”，如果未能连网获取时间，默认将从 2010 年 2 月 10 日 0 时 0 分 0 秒开始计时。

4.2 系统模式

TL-ER5120 路由器可以工作在 3 种模式下：NAT 模式、路由模式和全模式。

若TL-ER5120 需要作为网关应用在局域网与广域网之间，拓扑如图 4-5，可以将TL-ER5120 系统模式设为NAT模式；

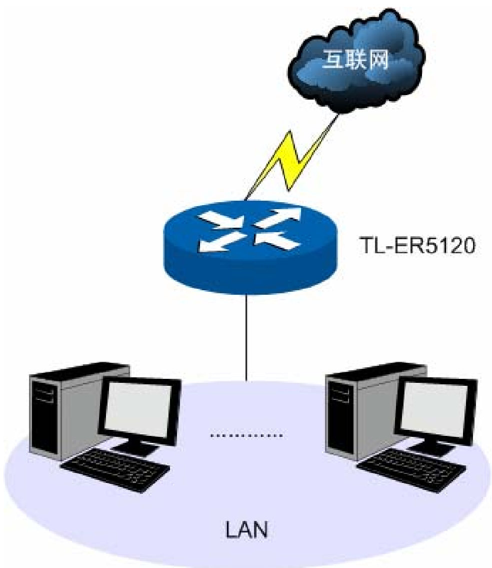


图 4-5 组网拓扑-NAT 模式

若TL-ER5120 在大型组网内用于连接两个不同区域的网络，这两个区域的主机都必须通过路由规则进行通信，拓扑如图 4-6，可以将TL-ER5120 系统模式设为路由模式；

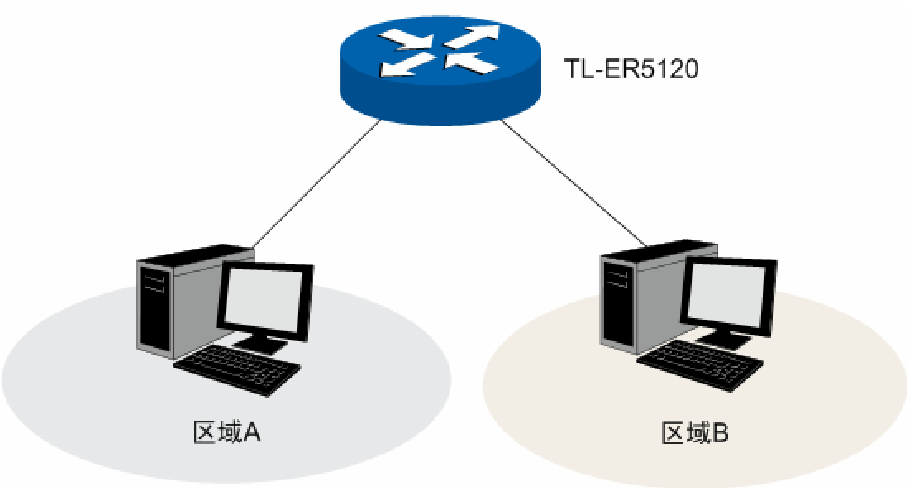


图 4-6 组网拓扑-路由模式

若TL-ER5120 应用于混合的组网拓扑中，如图 4-7，则可以将TL-ER5120 系统模式设为全模式。

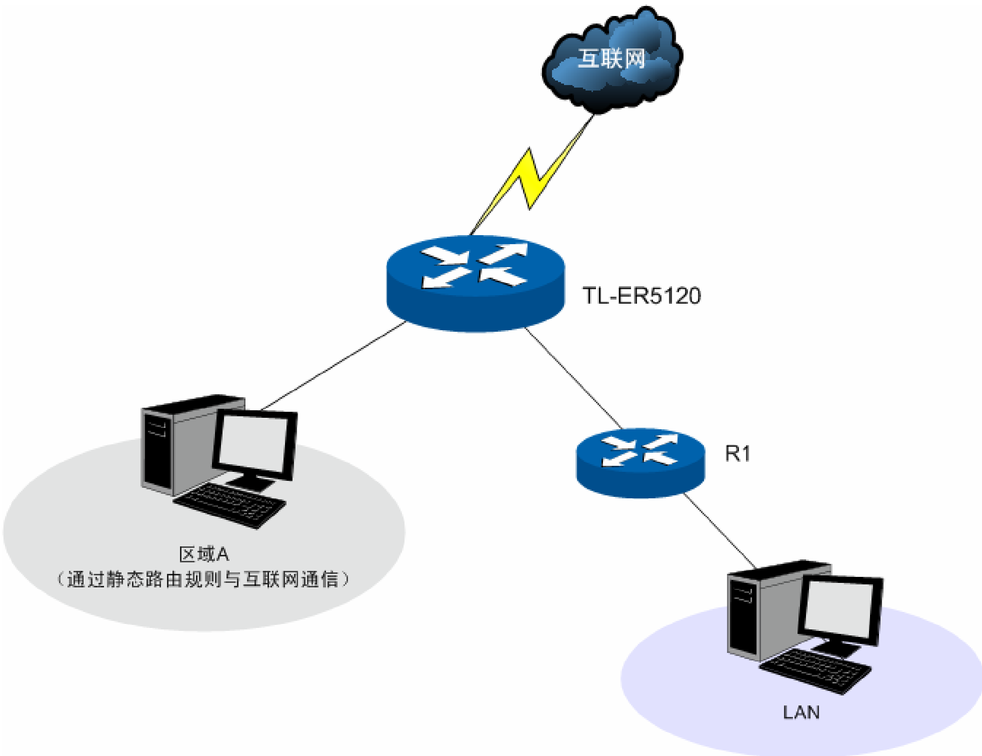


图 4-7 组网拓扑-全模式

界面进入方法：系统模式 >> 系统模式

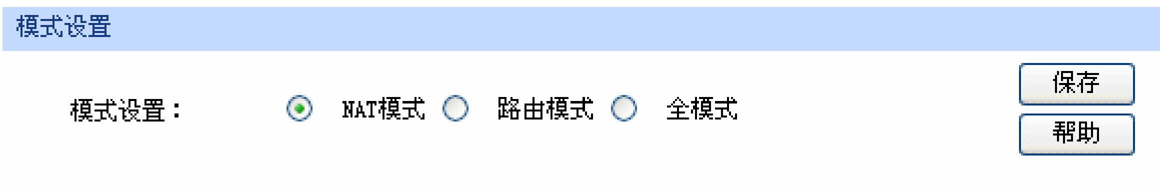


图 4-8 系统模式设置界面

请根据实际网络需要选择路由器的工作模式。

NAT 模式。此模式下，由局域网向广域网发送的数据包默认经过 NAT 转换，但路由器对所有源地址与局域网接口不在同一网段的数据包均不进行处理。例如，路由器 LAN 口 IP 设置为 192.168.1.1，子网掩码为 255.255.255.0，LAN 口所处网段为 192.168.1.0/24，此时，路由器收到源地址为 192.168.1.123 的数据包会进行 NAT 转换；但如果收到源地址为 20.31.76.80 的数据包则直接丢弃。

路由模式。此模式下，处于不同网段的主机可以通过相应的**路由设置**进行通信，但路由器不进行NAT转换。例如，当路由器DMZ口处于广域网模式时，DMZ区域内主机需要以路由方式访问广域网中的服务器，若静态路由规则允许，则可正常通信。此时，局域网内的主机不能访问广域网。

说明：

路由模式下，所有转发规则将失效。

全模式。全模式包含了 NAT 模式及路由模式，此模式下，路由器首先对符合 NAT 转发条件的数据包进行 NAT 转换；若不符合，则进行静态路由规则匹配，匹配成功的数据包以路由模式进行转发；匹配失败的数据包直接丢弃。这样，路由器既允许数据包进行 NAT 转换，也不阻隔与接口在不同网段的数据包。

4.3 接口设置

通过对 TL-ER5120 各接口的设置，可以帮助您快速连入互联网。

4.3.1 WAN模式

TL-ER5120 支持多种 WAN 口模式：单 WAN 口、双 WAN 口、三 WAN 口、四 WAN 口。

界面进入方法：接口设置 >> WAN 模式 >> WAN 模式

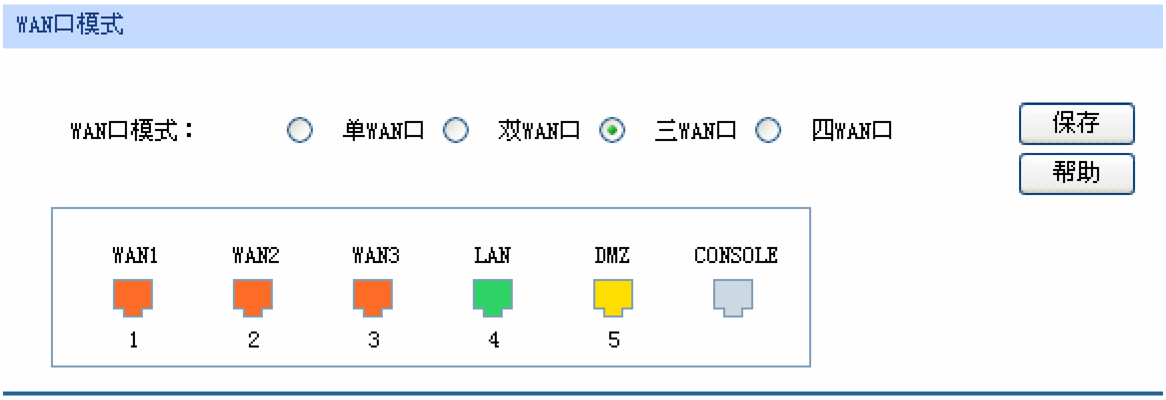


图 4-9 WAN 模式设置界面

请根据实际需求选择路由器的WAN模式。路由器会根据不同的WAN口模式对各物理端口做出相应配置，具体请参考图 4-9中的产品接口示意图。

注意：

TL-ER5120 出厂默认为双 WAN 口模式，切换 WAN 口模式可能导致配置信息丢失。若有重要配置信息，请在切换模式前备份。此外，若选择了四 WAN 口模式，DMZ 口将无法使用。

4.3.2 WAN设置

TL-ER5120 提供四种方式接入广域网：静态 IP、动态 IP、PPPoE、L2TP，请根据 ISP(Internet Service Provider, 网络服务提供商)提供的服务进行选择。

- 有线宽频一般使用动态 IP 连接方式；
- 光纤接入以及企业、网吧局域网内组网一般使用静态 IP 连接方式；
- xDSL 拨号上网则使用 PPPoE 连接方式；
- 虚拟专用拨号网络一般使用 L2TP 连接方式。

说明：

TL-ER5120 允许设置多个 WAN 口的 IP 地址为同一个网段，但需保证这些 WAN 口能连通到同一个网域，比如都连通到因特网或同一个局域网，否则可能会导致通信异常。

界面进入方法：**接口设置 >> WAN 设置 >> WAN 口设置**

1) 静态 IP 连接

若 ISP 提供了固定的 IP 地址，请选择静态 IP 手动配置 WAN 口参数。

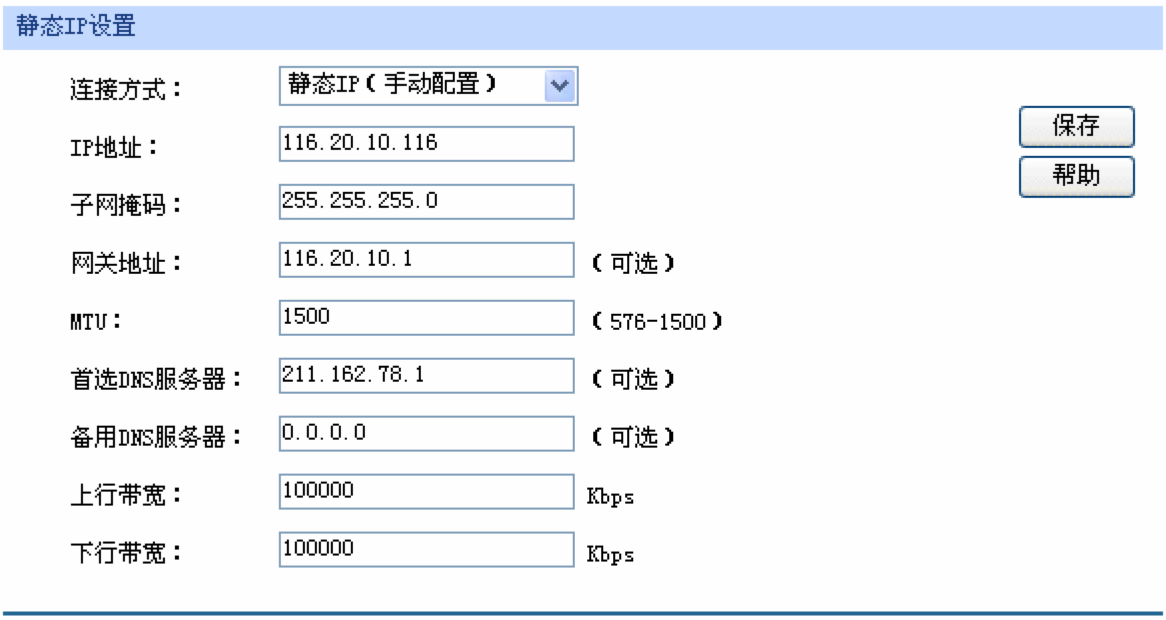


图 4-10 WAN 口设置界面-静态 IP

界面项说明：

- **静态 IP 设置**

连接方式	选择静态 IP 连接方式，进行手动配置。
IP 地址	设置路由器 WAN 口的 IP 地址。

子网掩码	设置路由器 WAN 口的子网掩码。
网关地址	设置网关地址。
MTU	MTU(Maximum Transmission Unit，最大传输单元)，可以设置数据包的最大长度。取值范围是 576-1500 之间的整数，默认值为 1500。若 ISP 未提供 MTU 值，请保持默认值不变。
首选 **DNS** 服务器	设置 DNS(Domain Name Server，域名解析服务器)地址，一般由 ISP 提供，如果留空，则无法通过域名访问互联网。
备用 **DNS** 服务器	设置备用 DNS 地址，一般由 ISP 提供，允许留空。
上行带宽	设置当前 WAN 接口数据流出的带宽大小。
下行带宽	设置当前 WAN 接口数据流入的带宽大小。

2) 动态 **IP** 连接

若 ISP 提供 DHCP 自动分配地址服务，请选择动态 IP 自动获取 WAN 口参数。



图 4-11 WAN 口设置界面-动态 IP

界面项说明：

- **动态 IP 设置**

连接方式	选择动态 IP 连接方式。点击<获取>得到 IP 参数，点击<释放>则不再使用现有 IP 参数。
主机名	输入用于标识路由器的名称。
MTU	MTU(Maximum Transmission Unit，最大传输单元)，可以设置数据包的最大长度。取值范围是 576-1500 之间的整数，默认值为 1500。若 ISP 未提供 MTU 值，请保持默认值不变。
手动设置 DNS 服务器	如果需要手动设置 DNS(Domain Name Server，域名解析服务)地址，请勾选此项。
首选 DNS 服务器	设置 DNS 地址，一般由 ISP 提供。
备用 DNS 服务器	设置备用 DNS 地址，一般由 ISP 提供，允许留空。
上行带宽	设置当前 WAN 接口数据流出的带宽大小。
下行带宽	设置当前 WAN 接口数据流入的带宽大小。

- **动态 IP 状态**

连接状态	显示当前 WAN 口 DHCP 分配状态。 “未启用”表示当前已选择动态 IP 连接方式但未保存生效； “正在连接”表示当前路由器正在向 ISP 获取 IP 参数； “已连接”表示路由器已成功获取 IP 参数； “未连接”表示路由器已发起请求，但未得到响应，请检查连接线路是否正常，若问题无法解决，请与 ISP 联系。
IP 地址	显示自动获取到的 IP 地址。
子网掩码	显示自动获取到的子网掩码。
网关地址	显示自动获取到的网关地址。
首选 DNS 服务器	显示 DNS 地址。
备用 DNS 服务器	显示备用 DNS 地址。

3) PPPoE 连接

若使用 xDSL/Cable Modem 拨号接入互联网，ISP 会提供上网帐号及密码，请选择 PPPoE 连接方式。



图 4-12 WAN 口设置界面-PPPoE

界面项说明：

➢ **PPPoE 设置**

连接方式　　选择 PPPoE。点击<连接>开始拨号并获取 IP 参数，点击<断开>则取消与互联网的连接同时释放已获取的 IP 参数。

帐号　　PPPoE 拨号的用户名，由 ISP 提供。

密码　　PPPoE 拨号的密码，由 ISP 提供。

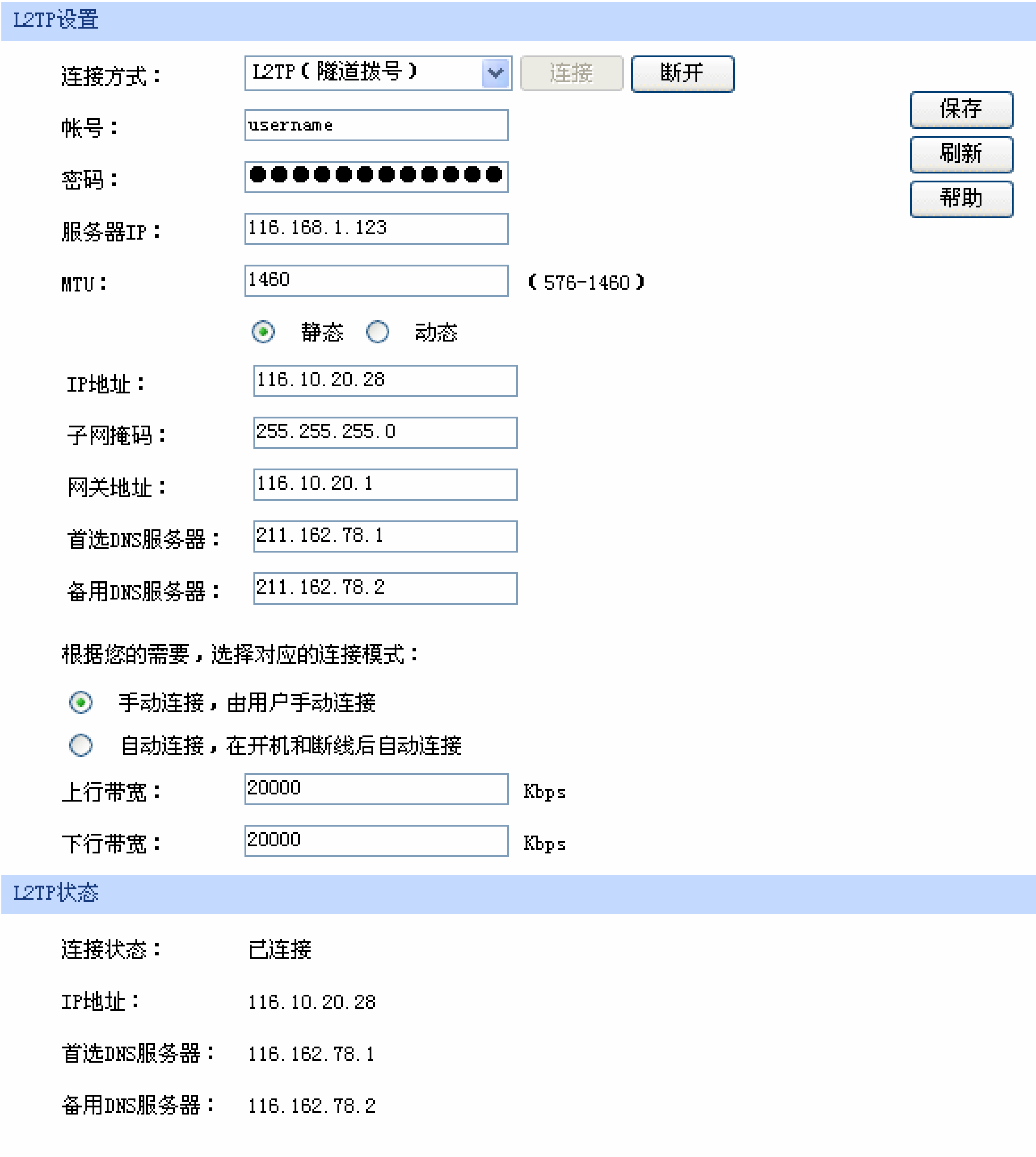
手动连接	用户可在需要上网时手动点击<连接>按钮连入互联网，适合按小时计费的拨号连接上网方式。
自动连接	每次接通路由器电源，路由器便自动拨号连入互联网，适合不限时间的包月计费拨号连接上网方式。
定时连接	设置连接时段，在此时段内路由器如果开启则自动拨号连接，适合用于需要限时上网的场合。
启用 PPPoE 高级设置	可以在此手动指定 MTU 值、服务名及 DNS(Domain Name Server，域名解析服务)地址。如果不清楚这些参数，请勿勾选此项。
MTU	MTU(Maximum Transmission Unit，最大传输单元)，可以设置数据包的最大长度。取值范围是 576-1492 之间的整数，默认值为 1480。若 ISP 未提供 MTU 值，请保持默认值不变。
服务名	输入服务名称，由 ISP 提供。
首选 DNS 服务器	设置 DNS 地址，一般由 ISP 提供。
备用 DNS 服务器	设置备用 DNS 地址，一般由 ISP 提供，允许留空。
上行带宽	设置当前 WAN 接口数据流出的带宽大小。
下行带宽	设置当前 WAN 接口数据流入的带宽大小。

➢ **PPPoE 状态**

连接状态	显示当前 WAN 口 PPPoE 拨号连接状态。 “未启用”表示当前已选择 PPPoE 拨号连接方式但未保存生效； “正在连接”表示当前路由器正在向 ISP 获取 IP 参数； “已连接”表示路由器已成功获取 IP 参数； “未连接”表示路由器已发起请求，但未得到响应，请检查用户名密码是否正确、连接线路是否正常，若问题无法解决，请与 ISP 联系。
IP 地址	显示通过 PPPoE 拨号后获取到的 IP 地址。
网关地址	显示通过 PPPoE 拨号后获取到的网关地址。
首选 DNS 服务器	显示 DNS 地址。
备用 DNS 服务器	显示备用 DNS 地址。

4) L2TP 连接

若使用虚拟专用拨号接入网络，ISP 会提供上网帐号及密码，请选择 L2TP 连接方式。



界面项说明：

➢ **L2TP 设置**

连接方式	选择 L2TP。点击<连接>开始拨号并获取 IP 参数，点击<断开>则取消与互联网的连接同时释放已获取的 IP 参数。
帐号	L2TP 拨号的用户名，由 ISP 提供。
密码	L2TP 拨号的密码，由 ISP 提供。
服务器 IP	L2TP 拨号的服务器的 IP 地址，由 ISP 提供。

MTU	MTU(Maximum Transmission Unit, 最大传输单元)，可以设置数据包的最大长度。取值范围是576-1460之间的整数，默认值为1460。若ISP未提供MTU值，请保持默认值不变。
静态/动态	选择静态或动态获取与L2TP服务器进行通信的IP地址。若选择静态方式，则需要手动设置IP地址；若选择动态，则外部的DHCP服务器将动态分配一个IP地址。
IP 地址	若选择静态，设置路由器WAN口的IP地址；若选择动态，显示路由器WAN口获取到的IP地址。
子网掩码	若选择静态，设置路由器WAN口的子网掩码；若选择动态，显示路由器WAN口获取到的子网掩码。
网关地址	若选择静态，设置网关地址；若选择动态，显示获取到的网关地址。
首选 DNS 服务器	若选择静态，设置DNS(Domain Name Server, 域名解析服务器)地址，一般由ISP提供，如果留空，则无法通过域名访问互联网；若选择动态，显示分配到的DNS地址。
备用 DNS 服务器	若选择静态，设置备用DNS地址，一般由ISP提供，允许留空；若选择动态，显示分配到的备用DNS地址。
手动连接	用户可在需要上网时手动点击<连接>按钮连入互联网，适合按小时计费的拨号连接上网方式。
自动连接	每次接通路由器电源，路由器便自动拨号连入互联网，适合不限时间的包月计费拨号连接上网方式。
上行带宽	设置当前WAN接口数据流出的带宽大小。
下行带宽	设置当前WAN接口数据流入的带宽大小。

➢ **L2TP 状态**

连接状态	显示当前WAN口L2TP拨号连接状态。 “未启用”表示当前已选择L2TP拨号连接方式但未保存生效； “正在连接”表示当前路由器正在向ISP获取IP参数； “已连接”表示路由器已成功获取IP参数； “未连接”表示路由器已发起请求，但未得到响应，请检查用户名密码是否正确、连接线路是否正常，若问题无法解决，请与ISP联系。
IP 地址	显示通过PPPoE拨号后获取到的IP地址。

首选 DNS 服务器　　显示 DNS 地址。

备用 DNS 服务器　　显示备用 DNS 地址。

4.3.3 LAN设置

4.3.3.1 LAN口设置

在此设置 TL-ER5120 路由器 LAN 口的 IP 参数。

界面进入方法：接口设置 >> LAN 设置 >> LAN 口设置

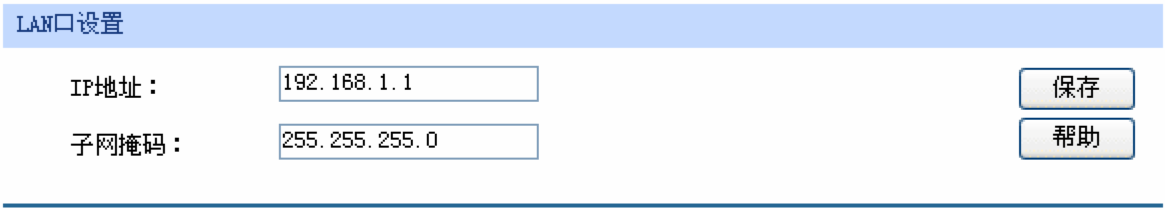


图 4-13 LAN 口设置界面

界面项说明：

➢ **LAN 口设置**

IP 地址　　设置路由器 LAN 口的 IP 地址，默认值为 192.168.1.1，可根据实际网络情况修改此值。局域网内部可通过该地址访问路由器。

子网掩码　　设置路由器 LAN 口的子网掩码，默认为 255.255.255.0，可根据实际网络情况修改此值。

注意：

若 LAN 口 IP 地址有修改，必须在保存配置后使用新的 LAN 口地址登录路由器 Web 管理界面。并且，局域网内所有计算机网关地址、子网掩码必须与修改后的 LAN 口设置保持一致，才能正常通信。

4.3.3.2 DHCP服务

DHCP(Dynamic Host Configuration Protocol，动态主机配置协议)。路由器具有 DHCP 服务功能，能够为所有接入 TL-ER5120 并且应用 DHCP 服务的网络设备自动分配 IP 参数。

界面进入方法：接口设置 >> LAN 设置 >> DHCP 服务

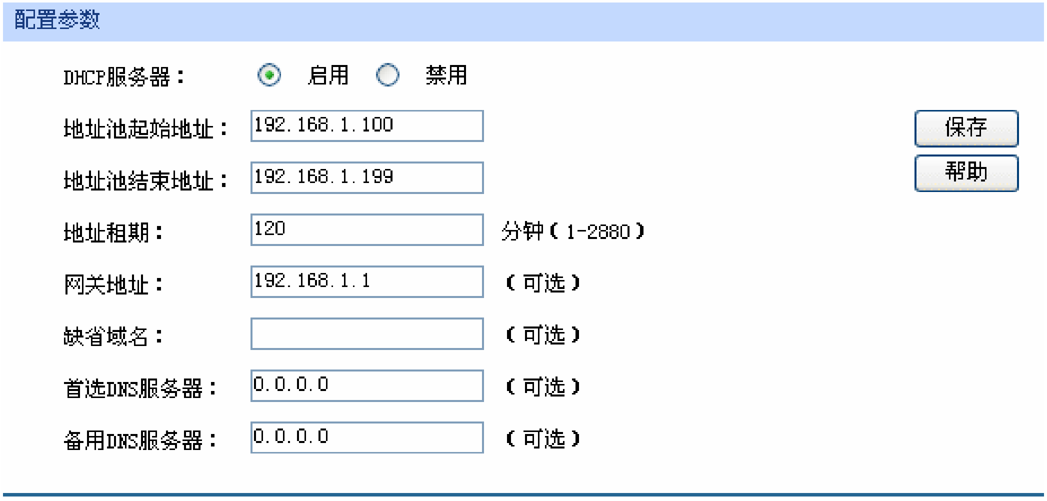


图 4-14 DHCP 服务设置界面

界面项说明：

➢ 配置参数

DHCP 服务器	选择开启或关闭 DHCP 服务。若希望路由器自动为计算机配置 TCP/IP 参数，请选择“启用”。
地址池起始地址	设置 DHCP 服务器自动分配 IP 地址的起始地址，该地址必须与 LAN 口 IP 地址设置在同一网段，默认值为 192.168.1.100。
地址池结束地址	设置 DHCP 服务器自动分配 IP 地址的结束地址，该地址必须与 LAN 口 IP 地址设置在同一网段，默认值为 192.168.1.199。
地址租期	设置 DHCP 分配地址有效时间，超时将重新分配。
网关地址	设置 DHCP 分配给客户端的网关地址，推荐设置为 LAN 口 IP 地址。
缺省域名	设置本地网域名，允许留空。
首选 DNS 服务器	设置 DNS 地址，推荐设为路由器 LAN 口 IP 地址，允许留空。
备用 DNS 服务器	设置备用 DNS 地址，允许留空。

4.3.3.3 客户端列表

客户端列表显示已由 DHCP 分配 IP 参数的主机信息。

界面进入方法：接口设置 **>> LAN** 设置 **>>** 客户端列表



图 4-15 客户端列表界面

可通过客户端列表查询 DHCP 客户端信息。如要获得最新 DHCP 服务分配的客户端信息，请点击<刷新>按钮。

4.3.3.4 静态地址分配

可根据接入设备的 MAC 地址手动分配 IP 地址。当对应的客户端设备请求 DHCP 服务器分配 IP 地址时，DHCP 服务器将自动为其分配指定的 IP 地址。

界面进入方法：接口设置 >> LAN 设置 >> 静态地址分配



图 4-16 静态地址分配设置界面

界面项说明：

➢ 静态地址

MAC 地址　　设置待分配 IP 地址的客户端的 MAC 地址。

IP 地址　　指定当前 MAC 地址所对应的客户端的 IP 地址。

备注　　添加对本条目的说明信息。

是否生效　　选择当前设置规则是否生效。

➢ 地址列表

在静态地址列表中，可以对已保存的静态 IP 地址分配规则进行相应操作。

图 4-16序号 1 规则的含义：MAC地址为 00-19-66-83-53-CF的客户端，指定其IP地址为 192.168.1.101，该规则未生效。

注意：

为了避免冲突，建议先进行IP MAC绑定，具体操作请参考**4.5.1ARP防护**，然后点击图 4-16静态地址分配设置界面中的<导入>按钮，直接获取IP MAC绑定列表中的静态地址条目。

4.3.4 DMZ设置

DMZ(Demilitarized Zone, 非军事区域)也称隔离区。TL-ER5120 提供一个物理 DMZ 接口，允许所有接入此端口的本地主机暴露在广域网中，进行一些特别的网络应用服务，如各种共享服务器、视频会议等。

DMZ 物理接口可以工作在两种模式下，广域网模式或局域网模式。

广域网模式中，DMZ 区域直接以路由模式与广域网之间通信。此时 DMZ 区域与广域网区域一样使用公有地址，不能主动访问局域网。

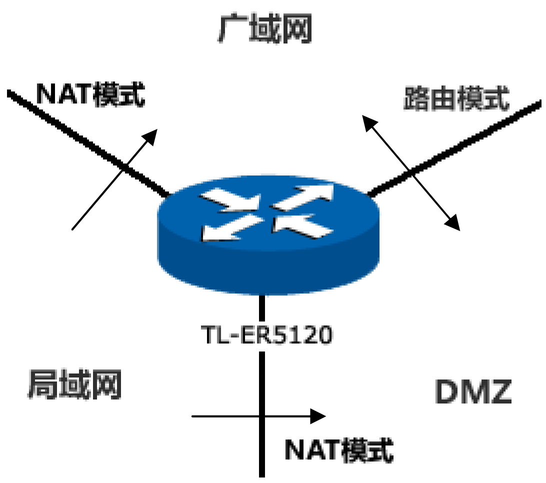


图 4-17 DMZ 口于广域网模式

局域网模式中，DMZ 区域访问广域网区域时需要经过 NAT 进行地址转换。此时 DMZ 区域可以使用与局域网区域不同网段的私有地址，并且可以主动向局域网区域发起访问连接。

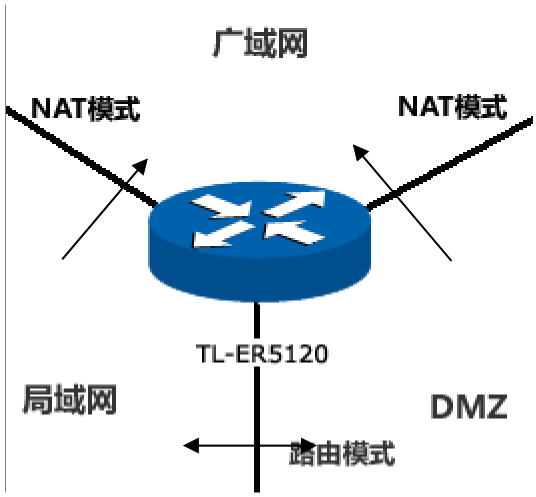


图 4-18 DMZ 口于局域网模式

4.3.4.1 DMZ口设置

在此控制 TL-ER5120 的 DMZ 口是否启用，并设置其 IP 参数。

界面进入方法：接口设置 **>> DMZ** 设置 **>> DMZ** 口设置

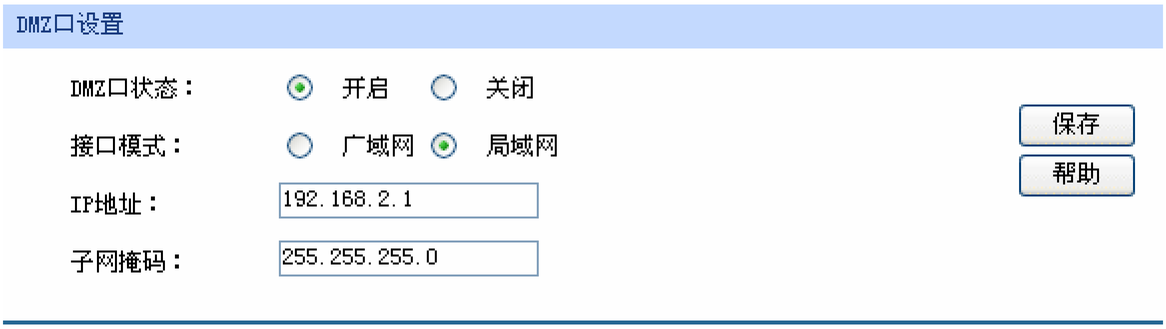


图 4-19 DMZ 口设置界面

界面项说明：

➢ **DMZ** 口设置

DMZ 口状态	设置是否启用 DMZ 口。在不启用的状态下，DMZ 口功能与 LAN 口功能相同。
接口模式	通过选择接口模式，可以控制 DMZ 区域与广域网、局域网之间的连接方式。
IP 地址	设置 DMZ 口的 IP 地址。
子网掩码	设置 DMZ 口的子网掩码。

说明：

DMZ口开启后将具有DHCP服务、客户端列表及静态地址分配功能设置，具体设置请参考第**4.3.3.2**至**4.3.3.4**小节。

注意：

当 DMZ 口开启并处于广域网模式时，若 ISP 为 DMZ 口提供的是单一广域网 IP 地址，请勿开启 DMZ 口的 DHCP 服务，否则 DMZ 区域内的主机分配到的地址不能正常访问广域网。若 ISP 提供的是地址段，请按照地址段范围设置 DHCP 地址池。

4.3.5 MAC设置

路由器 MAC 地址是它在网络中的身份标志，一般来说无需更改。

LAN 口 MAC 设置：

在一个所有设备都进行了 ARP 绑定的复杂拓扑中，如果其中一个网络节点的路由器更换为 TL-ER5120，为避免该节点下面接入的所有网络设备都更新 ARP 绑定表，直接将 TL-ER5120 的 LAN 口 MAC 地址设置为原路由器的 MAC 地址即可。

WAN 口 MAC 设置：

有些 ISP 要求上网帐号与拨号设备的 MAC 绑定，若此时拨号设备更换为 TL-ER5120，只需将路由器 WAN 口的 MAC 地址设置为原拨号设备的 MAC 地址即可。

DMZ 口 MAC 设置：

DMZ 口的 MAC 应用方式与 LAN 口类似。

界面进入方法：**接口设置 >> MAC 设置 >> MAC 设置**



图 4-20 MAC 设置界面

界面项说明：

➢ **MAC 设置**

接口	显示当前路由器各接口。
当前 MAC 地址	显示当前各接口的 MAC 地址。
设置	如需恢复初始状态，请点击<出厂 MAC>按钮。如需将当前 MAC 地址设置为管理主机 MAC 地址，即当前登录路由器进行配置管理的主机 MAC 地址，请点击<管理主机 MAC>按钮；该条目不出现在 LAN 口和 DMZ 口设置栏。

注意：

为了防止局域网内 MAC 地址冲突，路由器 LAN 口的 MAC 地址不能设置成当前管理主机的 MAC 地址。

4.4 转发规则

路由器通过 NAT(Network Address Translation，网络地址转换)技术，可以在局域网主机主动发起对广域网的访问时实现双方的互相通信。其原理是：当通信数据包经过 NAT 网关时，NAT 技术会将数据包中的 IP 地址在局域网地址与广域网地址间转换，同时也进行端口号的转换。

如今随着计算机的普及，广域网 IP 地址已经供不应求，通过 NAT 技术，局域网内所有主机在通信时可以使用一个广域网 IP 地址，而局域网内不同的主机使用不同的端口号，解决了 IP 地址紧缺的问题。

在应用了 NAT 及其扩展技术的网络环境中，局域网主机是不会直接被广域网主机发现的，因此 NAT 也为局域网提供了一定的网络安全保障，当有广域网主机需要主动访问局域网主机时，就必须通过转发规则来实现。

4.4.1 NAT映射

NAT 映射，可以将特定的局域网 IP 地址与指定的广域网 IP 地址唯一对应，多用于局域网内的服务器搭建。可在此设置 NAT 的端口范围和 NAT 映射关系。

界面进入方法：转发规则 >> NAT 映射



图 4-21 NAT 映射设置界面

界面项说明：

➢ **NAT 服务设置**

源端口范围　　设置作为 NAT 源端口的端口范围，范围跨度必须大于或等于 100。可设置范围为 2049-65000。

➢ **NAT 映射**

映射地址　　设置局域网 IP 地址和广域网 IP 地址的一对一映射。第一个输入框中应填写局域网 IP 地址，第二个输入框中应填写广域网 IP 地址。TL-ER5120 只允许 LAN 口到 WAN 口的映射。

出接口　　设定数据包发送出去的接口。

DMZ 转发　　勾选开启选项，DMZ 转发功能生效。可以将发送到映射后的地址的报文全部转发到映射前的地址主机。

备注　　添加对本条目的说明信息。

启用/禁用规则　　设置该条 NAT 映射条目是否生效。

➢ **映射列表**

在映射表中，可以对已保存的 NAT 映射条目进行相应设置。

图 4-21序号 1 条目的含义：局域网主机host1 的IP地址为 192.168.1.101，指定经NAT映射后的广域网IP地址为 222.135.48.52，数据包从WAN1 口发送出去，映射设置已启用。当host1 与广域网

通信时，从WAN1 口发出的数据包源IP地址将被NAT转换为广域网IP地址 222.135.48.52，而从广域网返回的数据包目的IP地址会被NAT转换为局域网IP地址 192.168.1.101。

注意：

NAT 映射只适用于 WAN 口使用静态 IP 连接方式的场合。若 WAN 口连接方式从静态 IP 切换为动态 IP、PPPoE 或 L2TP，以前设置的 NAT 映射都将失效，直接在动态 IP、PPPoE 或 L2TP 连接状态下设置的 NAT 映射也都不起作用。

4.4.2 多网段NAT

多网段 NAT，可以支持 LAN 或者 DMZ 接口下多个网段的 IP 通过 NAT 转换访问广域网。

界面进入方法：转发规则 >> 多网段 NAT



图 4-22 多网段 NAT 设置界面

界面项说明：

➢ 多网段 NAT 规则

网段地址	设置需要进行 NAT 转换的网段地址，以子网掩码值划分地址范围。
接口	在下拉列表中选择网段所在的接口，可选择 LAN 或者 DMZ。
启用/禁用规则	设置该条多网段 NAT 规则是否生效。
备注	添加对本条规则的说明信息。

➢ 规则列表

在规则列表中，可以对已保存的多网段 NAT 规则进行相应设置。

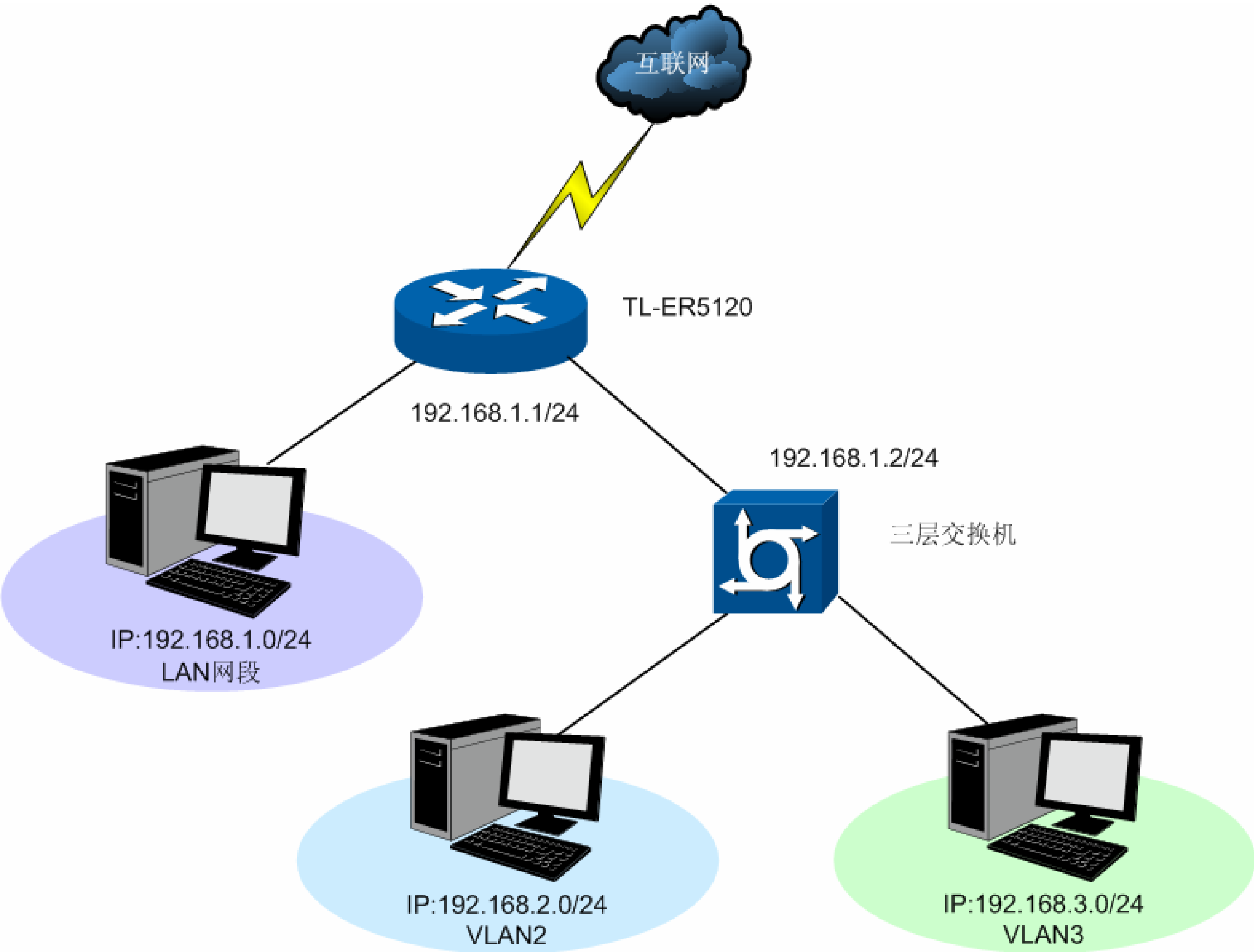
图 4-22序号 1 规则的含义：这是一条名为tplink1 的多网段NAT规则，路由器LAN口下的网段为172.31.80.0/24，本条规则已启用。在进行相应的静态路由规则设置后，该网段将可以通过本路由器进行NAT转换之后访问广域网。

注意：

- 多网段 NAT 功能需要同时配置静态路由才能生效。
- 只有当 DMZ 口开启时，DMZ 选项才在接口的下拉菜单中显示。
- 如果要指定所有 IP，其地址范围是“0.0.0.0 / 32”。
- 子网掩码值的相关设置请参考附录A 常见问题中的**问题 5**。

应用举例

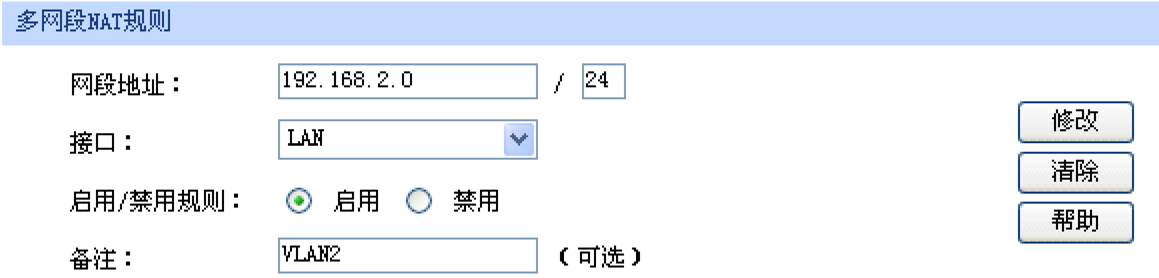
某网吧的网络结构如下：



TL-ER5120 的 LAN 网段为 192.168.1.0 /24，三层交换机下 VLAN2 网段为 192.168.2.0 /24，VLAN3 网段为 192.168.3.0 /24，三层交换机与 TL-ER5120 的 LAN 口级联 VLAN IP 为 192.168.1.2。现要实现 VLAN2 和 VLAN3 网段可以访问互联网。

可以通过如下设置来实现：

1. 首先设置多网段 NAT 规则，分别添加 VLAN2 与 VLAN3 的网段地址。



设置完成后的规则如下：

规则列表

选择	序号	网段地址	接口	状态	备注	设置
☐	1	192.168.2.0/24	LAN	已启用	VLAN2	
☐	2	192.168.3.0/24	LAN	已启用	VLAN3	

全选 启用 禁用 删除 搜索

2. 然后设置相应的静态路由规则，指定下一跳为网段地址所属三层交换机与本路由器 LAN 口直接相连的接口 IP。

界面进入方法：路由设置 >> 静态路由



设置完成后的静态路由如下：

规则列表

选择	序号	目的地址	子网掩码	下一跳	出接口	状态	备注	设置
☐	1	192.168.2.0	255.255.255.0	192.168.1.2	LAN	已启用	VLAN2	
☐	2	192.168.3.0	255.255.255.0	192.168.1.2	LAN	已启用	VLAN3	

全选 启用 禁用 删除 搜索

4.4.3 虚拟服务器

在路由器默认设置下，广域网中的主机不能直接与局域网主机进行通信。为了方便广域网的合法用户访问本地主机，又要保护局域网内部不受侵袭，路由器提供了虚拟服务器功能。

可以通过虚拟服务器定义一个服务端口，并以 IP 地址指定其对应的局域网服务器，则广域网所有对此端口的服务请求都将被重定位到该服务器上。这样广域网的用户便能成功访问局域网中的服务器，同时不影响局域网内部的网络安全。

界面进入方法：转发规则 >> 虚拟服务器



图 4-23 虚拟服务器设置界面

界面项说明：

➢ **NAT DMZ 服务**

NAT DMZ 服务　　设置是否启用 NAT DMZ 服务。NAT DMZ 是 NAT 应用的一种特殊服务，相当于一条默认的转发规则。若主机开启了 NAT DMZ 服务，路由器会将所有由广域网发起的、不符合所有现有连接和转发规则的数据全部转发至指定的主机。

主机地址　　指定作为 NAT DMZ 服务器的主机 IP 地址。

➢ **虚拟服务**

服务名称　　用户自定义，标识一条虚拟服务器规则。名称长度需在 28 个字符以内，中英文均可，一个中文占用 2 个字符空间。

外部端口	为本条虚拟服务器规则指定路由器提供给广域网的服务端口或端口范围，广域网对该端口或端口范围的访问都将被重定位到局域网中指定的服务器。
内部端口	指定局域网内虚拟服务器主机的实际服务端口。
服务协议	指定应用本条虚拟服务器规则的数据包协议类型。
内部服务器 IP	为本条虚拟服务器规则指定局域网服务器的 IP 地址。广域网对局域网指定端口的访问都将发送到该主机。
启用/禁用规则	设置是否应用本条虚拟服务器规则。

注意：

- 外部端口与内部端口的取值范围均为 1-65535 之间的任意整数。
- 不同虚拟服务器规则的外部端口取值不能相同，内部端口取值可相同。

➢ 服务列表

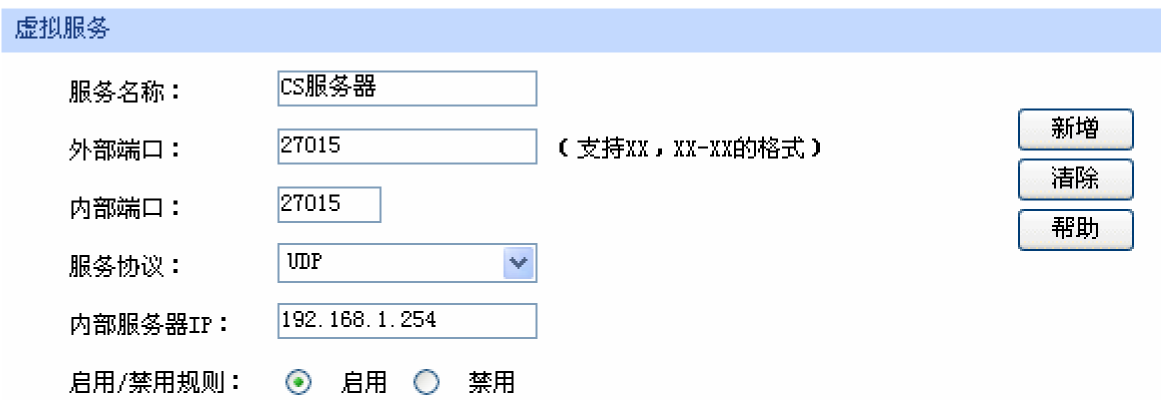
在服务列表中，可以对已保存的虚拟服务器规则进行相应设置。

图 4-23序号 1 规则的含义：这是一条名为apply1 的虚拟服务器规则，由广域网向路由器端口 8080 发起的TCP数据都将转发到局域网IP地址为 192.168.1.102 主机的 80 端口上，本条规则已启用。

应用举例

某网吧在局域网内的游戏服务器 192.168.1.254 上搭建了 CS 服务器，CS 服务器使用的是 UDP 27015 端口，现要实现广域网的玩家能连接到局域网内的这台服务器上联机游戏。

可以通过虚拟服务器实现这个需求。首先需要添加虚拟服务器规则，将路由器外部端口 27015 映射到内网 CS 服务器 192.168.1.254 的 UDP 端口 27015 上，使用的服务协议是 UDP 协议，设置如下图。点击<新增>按钮保存设置。设置完成后，广域网的玩家就可以连接到网吧局域网内的 CS 服务器进行游戏了。



4.4.4　端口触发

由于防火墙的存在，一些如网络游戏、视频会议、网络电话、P2P 下载等应用程序需要通过设置转发规则才能正常工作，而这些应用程序又要求多个端口连接，针对单一端口的虚拟服务器功能已不能满足需求，此时就需要使用端口触发功能。

当一个应用程序向触发端口发起连接时，对应开放端口中的所有端口就会打开，以备后续连接。

界面进入方法：转发规则 >> 端口触发



图 4-24 端口触发设置界面

界面项说明：

➢　端口触发

服务名称	用户自定义，标识一条端口触发规则。名称长度需在 28 个字符以内，中英文均可，一个中文占用 2 个字符空间。
触发端口	应用程序首先发起连接的端口。只有该端口发起连接时，对应开放端口中的所有端口才可以开放，并为应用程序提供服务，否则开放端口中的所有端口是不会开放的。
触发协议	设定在触发端口上使用的数据包协议类型。
开放端口	为应用程序提供服务的一个或多个端口。当触发端口上发起连接后，开放端口打开，之后应用程序便可以通过这些开放端口发起后续连接。
开放协议	设定在开放端口上使用的数据包协议类型。
启用/禁用规则	设置是否应用本条端口触发规则。

注意：

- 触发端口与开放端口的取值范围均为 1-65535 之间的任意整数。开放端口取值可以指定一个连续的范围，如 8690-8696。
- 路由器支持 16 条端口触发规则，每条规则最多支持 5 组开放端口，每条规则的开放端口数总和需小于或等于 100。

➢ 触发列表

在触发列表中，可以对已保存的端口规则进行相应设置。

图 4-24序号 1 规则的含义：这是一条名为apply1 的端口触发服务规则，当局域网内发起端口为5354 的TCP访问时，对TCP和UDP协议开放 5355-5358 端口。

4.4.5 ALG服务

ALG(Application Layer Gateway, 应用层网关)。为了保证一些应用程序的正常使用，请开启 ALG 服务。

界面进入方法：转发规则 >> ALG 服务



图 4-25 ALG 服务设置界面

界面项说明：

➢ **ALG 服务**

FTP ALG 服务　　选择启用或禁用 FTP ALG 服务，默认为启用，如无特殊需求请保持默认配置不变。

H.323 ALG 服务　　选择启用或禁用 H.323 ALG 服务，默认为启用，如无特殊需求请保持默认配置不变。H.323 多媒体协议多用于视频会议、IP 电话等场合。

IPsec ALG 服务　　选择启用或禁用 IPsec ALG 服务，默认为启用，如无特殊需求请保持默认配置不变。

PPTP ALG 服务　　选择启用或禁用 PPTP ALG 服务，默认为启用，如无特殊需求请保持默认配置不变。

4.5 安全策略

安全策略主要用于防御当今互联网环境中多种类型的攻击，并消除潜在的安全隐患。

4.5.1 ARP防护

一台主机向局域网内另一台主机发送 IP 数据包，此时设备需要通过 MAC 地址确定目的接口才能进行通信，而 IP 数据包中不包含有 MAC 地址信息，因此需要将 IP 地址解析为 MAC 地址。ARP（Address Resolution Protocol，地址解析协议）正是用来实现这一目的的网络协议。

网络中的所有设备，包括路由器和计算机在内，都各自维护一份 ARP 列表，该列表建立了主机 IP 地址和 MAC 地址一一对应关系。按照 ARP 协议的设计，主机也会接收不是自己主动请求的 ARP 应答，并将应答的 IP 地址和 MAC 地址添加到 ARP 表中。每次通信时会先通过该列表查找对应地址，减少网络上过多的 ARP 通信量，但同时也为“ARP 欺骗”创造了条件。

ARP 欺骗是局域网的攻击主机发送 ARP 欺骗包，将伪造的 IP 与 MAC 对应关系替换设备 ARP 列表中的记录，就会导致局域网内计算机不能正常上网。这类 ARP 攻击严重影响了局域网内部通信，由此便产生了 ARP 防护技术。

4.5.1.1 IP MAC绑定

IP MAC 绑定是一种防护技术，能够防止 ARP 列表被伪造的 IP MAC 对应信息替换。

界面进入方法：安全策略 **>> ARP 防护 >> IP MAC 绑定**



图 4-26 IP MAC 绑定设置界面

界面项说明：

➢ 功能设置

推荐勾选所有项目，以便最大程度地防范 ARP 攻击。在勾选“仅允许 IP MAC 绑定的数据包通过路由器”选项前，请先将管理主机的 IP MAC 信息导入绑定列表中，并设置生效。

当路由器受到 ARP 攻击时，路由器会将自身正确的 ARP 列表信息以 GARP(Gratuitous ARP, 免费 ARP)包的方式主动发送给被攻击的设备，从而替换该设备错误的 ARP 列表信息。可在发包间隔处指定发包速率。

勾选“启用ARP日志记录”后路由器会将ARP日志发送到指定的日志服务器中。日志服务器即4.1.3日志中设置的服务器地址。

➢ IP MAC 绑定

IP 地址	手动输入需要进行绑定的 IP 地址。
MAC 地址	手动输入与 IP 地址正确对应的 MAC 地址。
备注	添加对本条目的说明信息。
是否生效	设定当前绑定条目是否生效。

➢ 绑定列表

在绑定列表中，可以对已保存的 ARP 绑定条目进行相应设置。

图 4-26序号1条目的含义：目前路由器已将IP地址192.168.1.101与MAC地址00-19-66-83-53-CF进行绑定，该绑定规则已生效。

注意：

若当前绑定列表中所有条目都未生效，在勾选“仅允许 IP MAC 绑定数据包通过路由器”的功能设置选项并保存后，将无法登录路由器 Web 管理界面，此时必须将路由器恢复出厂配置才能再次登录。

4.5.1.2 ARP扫描

ARP 扫描界面可以将指定范围内的 IP 与其对应 MAC 地址全部扫描出来，在扫描列表中显示。

界面进入方法：安全策略 **>> ARP 防护 >> ARP 扫描**

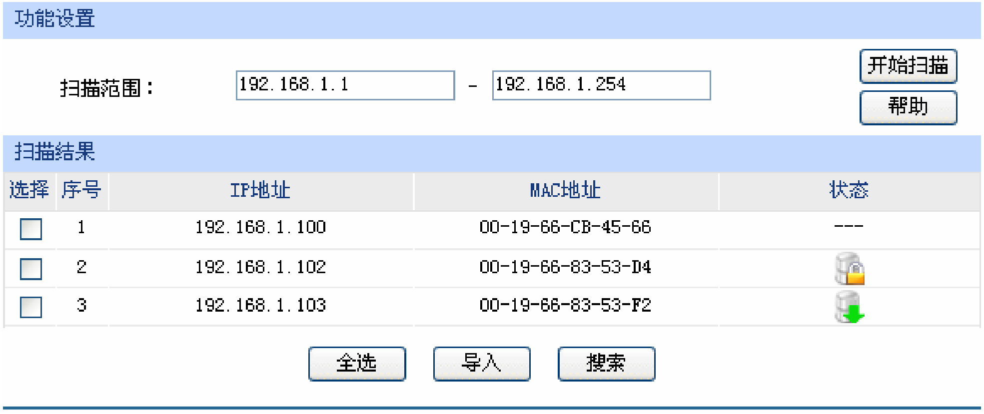


图 4-27 ARP 扫描界面

在扫描范围填入起始 IP 与结束 IP 后，点击<开始扫描>按钮，路由器将扫描该范围内所有正在工作的主机，并将它们对应的 IP MAC 地址信息显示在扫描列表中。

扫描结果中显示的 IP MAC 地址对应信息条目并不代表已经被绑定，在“状态”一列中会标识当前状态：

符号“---”表示当前条目未被绑定，可能会被错误的 ARP 信息更替掉；

图片表示当前条目已导入“IP MAC 绑定”界面的绑定列表中，但还未绑定生效；

图片表示当前条目已进行绑定，可以防御 ARP 攻击。

若现在需要绑定扫描列表中未绑定的条目，可以在“选择”一列勾选这些条目，然后点击<导入>按钮，在与已绑定条目不冲突的情况下，导入后绑定立即生效。

注意：

若局域网内已经存在 ARP 攻击导致部分主机通信异常，则不可通过扫描方式添加绑定，请在“IP MAC 绑定”界面进行手动绑定。

4.5.1.3 ARP列表

路由器会将曾经与其通信过的主机 IP MAC 对应信息保存在 ARP 列表中。

界面进入方法：安全策略 **>> ARP** 防护 **>> ARP** 列表

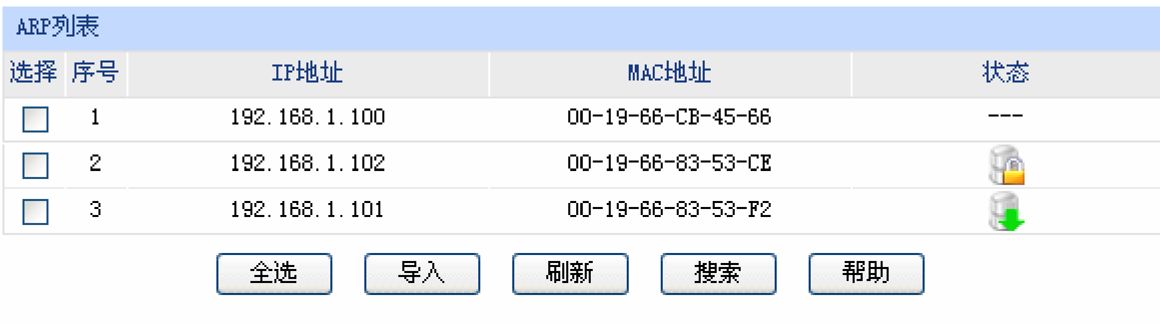


图 4-28 ARP 列表界面

ARP列表条目的操作可参考**4.5.1.2 ARP扫描**的扫描列表。

列表中未绑定的条目并不是一直存在，除了会被新的 IP MAC 对应信息更替之外，还会由于长时间未通信而自动从列表中删除，这个时间段就是 ARP 信息的老化时间。

4.5.2 访问控制

访问控制是一种针对 IP 地址和端口的过滤方式，合理设置访问控制可以消除潜在的安全隐患。

4.5.2.1 访问规则

界面进入方法：安全策略 >> 访问控制 >> 访问规则



图 4-29 访问规则设置界面

界面项说明：

➢ 访问规则

策略类型	在下拉列表中选择适用于本条规则的策略类型，可选择阻塞或者允许。若选择阻塞，则符合该条规则的所有数据包将无法通过路由器；若选择允许，则符合该条规则的数据包能通过路由器。
服务类型	在下拉列表中选择本条规则所针对的服务类型，不属于指定范围内的服务将不会应用过滤规则。例如在策略为阻塞的前提下，只选定了FTP一种服务类型时，其他服务类型的数据包仍旧可以通过路由器。如果列表中没有合适的服务类型，可以参见**4.5.2.2服务类型**进行添加，可通过下拉列表旁边的<服务类型>按钮快速进入设置界面。
生效接口域	在下拉列表中选择本条规则所针对的接口域，可选择 WAN 或者 LAN 或者 DMZ。选择 WAN（或者 LAN 或者 DMZ）时表示所有 WAN（或者

	LAN 或者 DMZ）接口。当接收报文的接口为指定接口域时，该规则生效。
源地址范围	输入需要管理的地址，以子网掩码值划分地址范围。
目的地址范围	输入需要限制访问的地址，以子网掩码值划分地址范围。
规则生效时间表	指定规则生效时间，其他时间规则不生效。时间以 24 小时制进行设定，精确到分钟，下方可勾选生效的日期，以一周为单位。
备注	添加对本条规则的说明信息。
指定位置	勾选该项后，可以将当前设置的条目添加到访问规则列表中指定序号的位置。默认情况下，规则新增生效后会显示在访问规则列表的最后。

➢ 规则列表

在规则列表中，可以对已保存的访问规则进行相应设置。在规则列表中，序号数字越小的规则，执行的优先级越高。

图 4-29序号 1 规则的含义：192.168.1.0/24 网段的主机在一周中的每天 08:00-24:00 时间范围内向广域网 116.10.1.0/24 网段发送的ICMP服务数据包将无法通过路由器。

说明

- 局域网内没有设置规则的 IP 段，默认的策略类型是允许。
- 如果要指定所有 IP，其地址范围是“0.0.0.0 / 32”。
- 子网掩码值的相关设置请参考附录A 常见问题中的**问题 5**。
- 只有当 DMZ 口开启时，DMZ 选项才在生效接口域的下拉菜单中显示。

4.5.2.2 服务类型

为了能够在定制防火墙策略时比较方便地指定需要过滤的协议和端口号，设备提供了服务类型管理功能。每一个服务类型由协议类型和端口范围两部分构成。系统已经预定义了如 HTTP、FTP、TELNET 等常用服务类型，也可以根据需要添加自定义服务类型。

界面进入方法：安全策略 >> 访问控制 >> 服务类型



选择	序号	服务名称	协议类型	目的端口范围	设置
	1	ICMP	ICMP	N/A	---
	2	FTP	TCP	21	---
	3	SSH	TCP	22	---
	4	TELNET	TCP	23	---
	5	SMTP	TCP	25	---
	6	DNS	UDP	53	---
	7	HTTP	TCP	80	---
	8	POP3	TCP	110	---
	9	SNTP	UDP	123	---
	10	H.323	TCP	1720	---

图 4-30 服务类型设置界面

界面项说明：

➢ 服务类型

服务名称 用户自定义，标识一条服务类型。名称长度需在 28 个字符以内，中英文均可，一个中文占用 2 个字符空间。该名称将显示在“访问规则”设置的服务类型下拉列表中。

协议类型 设置协议类型，可供用户定义的协议类型有 TCP、UDP、TCP/UDP。

目的端口范围 设定该服务所使用的端口号范围。起始端口号不能大于结束端口号。

➢ 服务列表

在服务列表中，可以对自定义的服务类型条目进行相应设置。

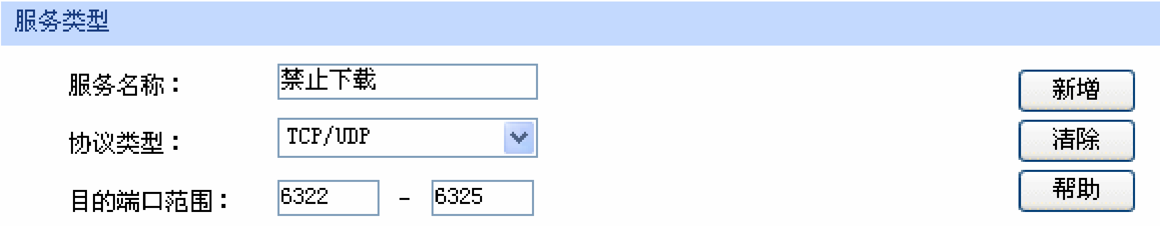
注意：

系统预定义的服务类型不可进行配置操作。

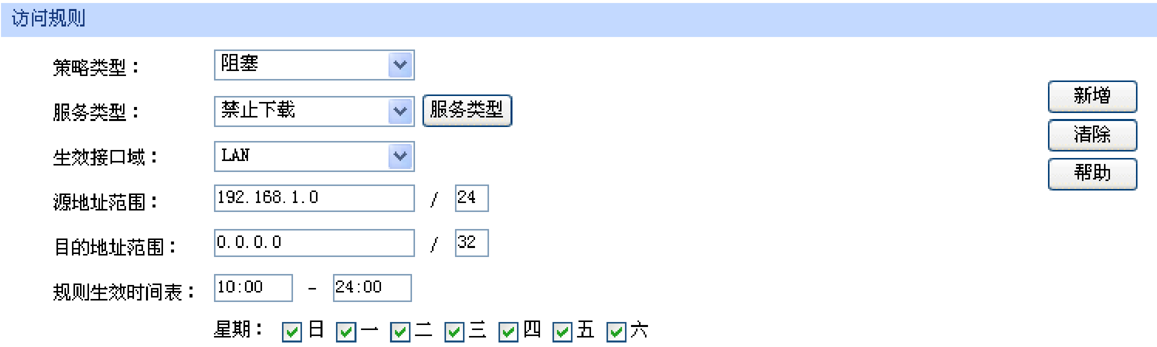
应用举例

需求：某网吧为使网络顺畅运行，希望实现在上网高峰期（每天上午 10 点到晚上 24 点）禁止某下载工具（端口 6322-6325）的使用，而在其它时间不限制该下载工具的使用。

此需求依旧可以通过设置访问规则来实现。首先，同样需要新增一个服务类型，设置 6322-6325 为服务端口，设置完成后点击<新增>按钮保存生效。



选择刚设置的“禁止下载”服务类型，新增一条禁止局域网通过 6322-6325 端口访问广域网的访问规则。最后点击<新增>按钮保存生效，完成设置。



4.5.3 攻击防护

攻击防护可防止广域网对路由器或局域网内计算机进行端口扫描和恶意攻击，以此来保证它们的安全运行。

界面进入方法：安全策略 >> 攻击防护 >> 攻击防护

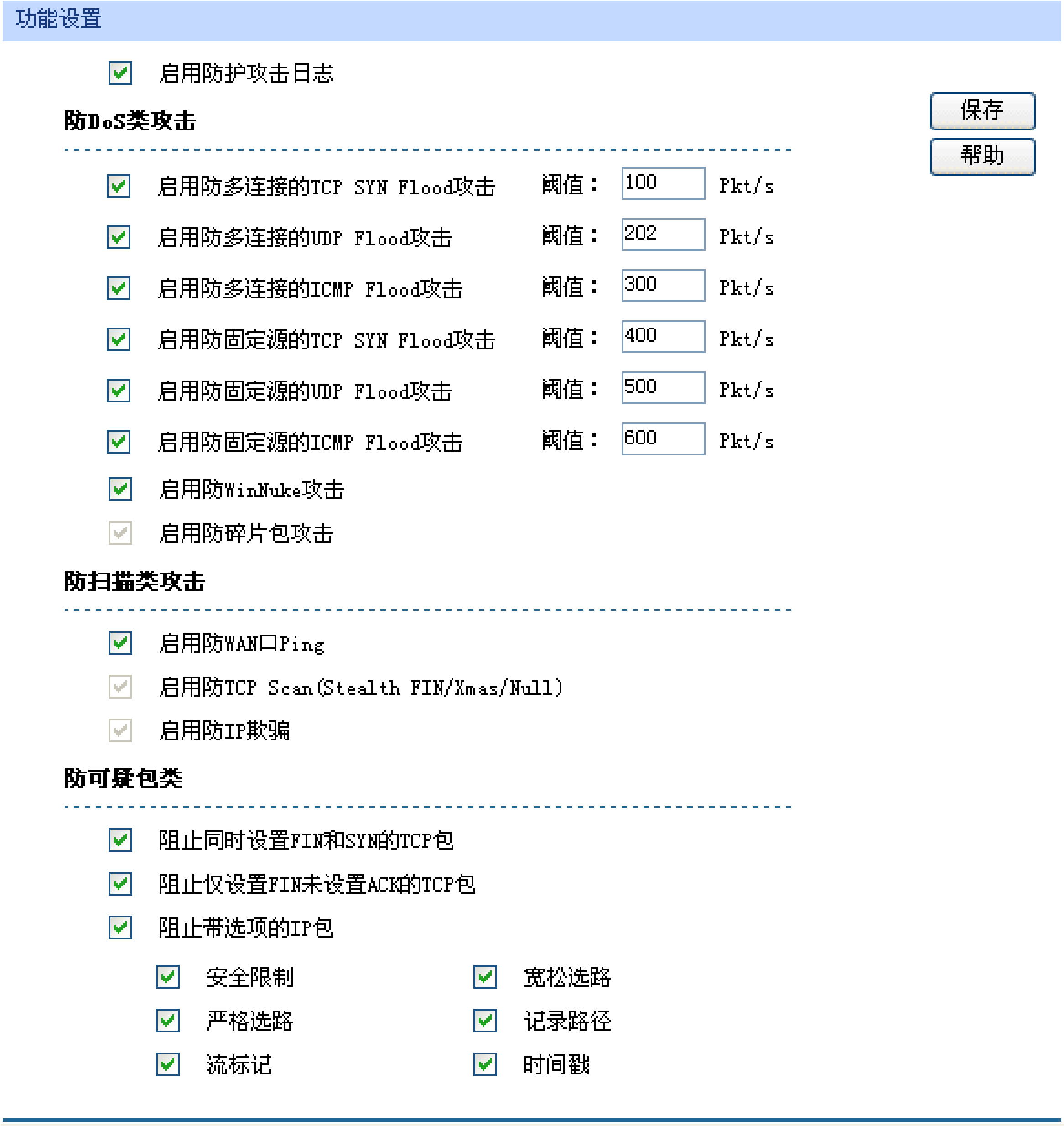


图 4-31 攻击防护设置界面

界面项说明：

➢ 功能设置

启用防护攻击日志　　勾选此项后路由器会记录相关的防护日志。

防 DoS 类攻击　　DoS(Denial of Service，拒绝服务)是一种利用发送大量的请求服务占用过多的资源，让目的路由器和服务器忙于应答请求或等待不存在的连接回复，而使正常的用户请求无法得到响应的攻击方式。常使用的 DoS 攻击为洪水攻击，包括 TCP SYN，UDP，ICMP 等。推荐勾选界面上所有防 DoS 攻击选项。

防扫描类攻击　　扫描一般是发起攻击的第一步，攻击者可以利用各种扫描手段来获取目标网络的主机信息及端口开放情况，便于发起下一步攻击。推荐勾选界面上所有防扫描类攻击选项。

防可疑包类	可疑包即非正常数据包，有可能是病毒或攻击者的试探。推荐勾选界面上所有防可疑包选项。

4.5.4 接入过滤

接入过滤是针对 MAC 地址和 URL 地址的过滤方式，与其他安全策略共同配合，保护局域网安全。

4.5.4.1 MAC过滤

在此可以通过指定 MAC 地址对部分局域网主机进行过滤。

界面进入方法：安全策略 >> 接入过滤 >> MAC 过滤



图 4-32 MAC 过滤设置界面

界面项说明：

➢ 功能设置

若需要严格控制局域网内某些计算机访问广域网，推荐勾选“启用 MAC 地址过滤功能”，并根据实际情况选择一种过滤规则。

➢ MAC 地址过滤规则

MAC 地址	输入需要控制的局域网主机 MAC 地址。
备注	添加对本条规则的说明信息。

➢ 规则列表

在规则列表中，可以对已保存的 MAC 地址条目进行相应设置。

4.5.4.2 URL过滤

URL(Uniform Resource Locator，统一资源定位符)，即广域网中标识资源位置的网络地址。URL 过滤能够实现对广域网网址的过滤，方便对局域网访问广域网的通信进行管理。

界面进入方法：安全策略 >> 接入过滤 >> URL 过滤

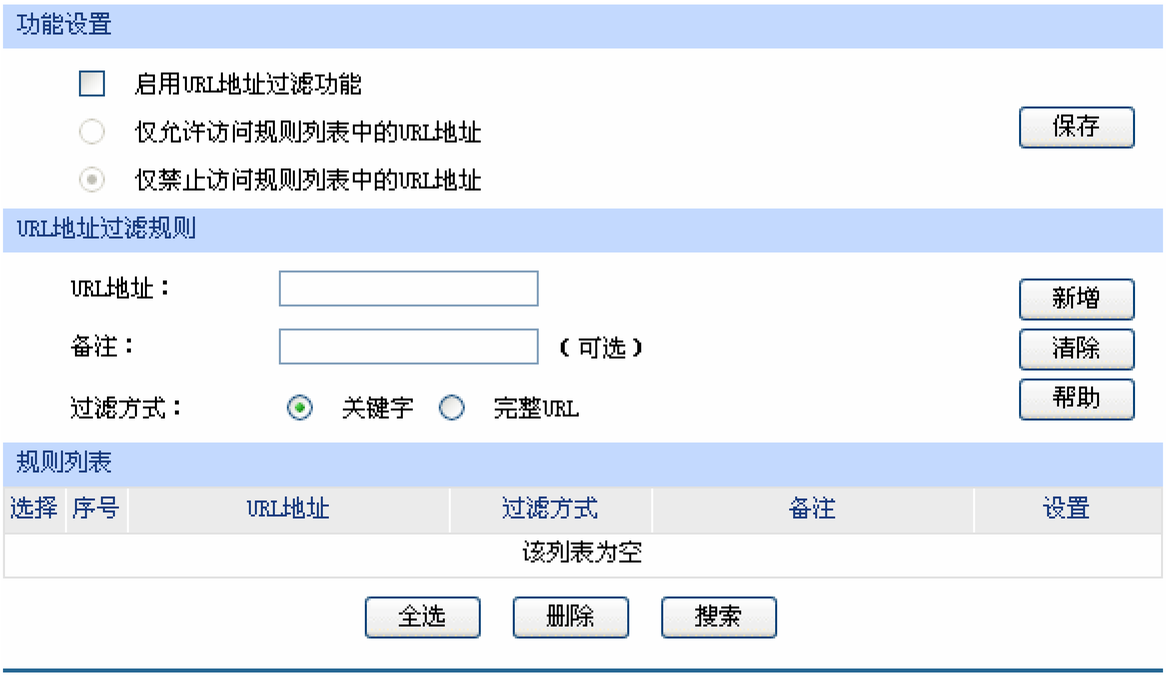


图 4-33 URL 过滤设置界面

界面项说明：

➢ 功能设置

若需要严格控制局域网对广域网的访问，推荐勾选“启用 URL 地址过滤功能”，并根据实际情况选择一种过滤规则。

➢ URL 地址过滤规则

URL 地址	输入指定的关键字字符，或完整的广域网 URL 地址。
备注	添加对本条规则的说明信息。
过滤方式	选择一种过滤方式。“关键字”过滤即所有包含指定字符的 URL 地址全都进行过滤；“完整 URL”过滤则仅当 URL 地址完全匹配您输入的完整 URL 地址时才能进行过滤。

➢ 规则列表

在规则列表中，可以对已保存的 URL 地址条目进行相应设置。

应用举例

某网吧希望禁止局域网内的主机访问网站：www.aabbcc.com，同时还禁止下载“.exe”后缀的文件。

可以通过设置 URL 过滤实现此需求。您需要设置完整 URL 过滤“www.aabbcc.com”，以及关键字过滤“.exe”，如下图，设置完成后点击<新增>按钮保存生效。



4.6 传输控制

传输控制功能主要对带宽和连接数进行控制，以保证网络通信质量。

4.6.1 带宽控制

带宽控制功能通过对各种数据流设置相应的限制规则，实现对数据传输的带宽控制，从而使有限的带宽资源得到合理分配，达到有效利用现有带宽的目的。

4.6.1.1 综合设置

可以在此限定各接口间互相发送数据包的最大带宽及预留带宽。

界面进入方法：传输控制 >> 带宽控制 >> 综合设置



图 4-34 综合设置界面

界面项说明：

➢ 功能设置

不启用带宽控制　　勾选此项时，所有带宽控制设置均不生效。

启用普通带宽控制　　勾选此项以启用普通带宽控制功能。

启用智能带宽控制　　勾选此项以启用智能带宽控制功能。当带宽利用率达到指定的值时，带宽控制功能生效。

➢ 各接口带宽

接口　　显示路由器当前已启用的 WAN 口，以及总 WAN 口。总 WAN 口的带宽为已启用接口带宽之和。

上行带宽　　设置对应WAN口数据流出的带宽上限，如需调整，请至**WAN设置**页面修改相应WAN口参数。

下行带宽　　设置对应WAN口数据流入的带宽上限，如需调整，请至**WAN设置**页面修改相应WAN口参数。

➢ 默认规则带宽

数据流向	“上行”表示由局域网发送数据到广域网，如局域网内计算机向广域网上的 FTP 服务器上传文件；“下行”表示由广域网发送数据到局域网，如局域网内计算机从广域网上的 FTP 服务器下载文件。
最小保证带宽	设置对应数据流向的带宽下限。
最大限制带宽	设置对应数据流向的带宽上限。

说明：

- WAN 口的出入带宽必须小于或者等于 ISP 提供的参数。如果超过实际物理带宽，则带宽控制功能失效。
- 若有数据由 A 接口流入路由器后由 B 接口流出，而 A 接口入口带宽与 B 接口出口带宽不同时，以两者带宽的最小值为有效带宽。

4.6.1.2 带宽控制规则

可以在此设置带宽控制规则的参数。

界面进入方法：传输控制 >> 带宽控制 >> 带宽控制规则



图 4-35 带宽控制规则设置界面

界面项说明：

- 带宽控制规则

数据流向	选择控制规则的数据流向。箭头方向代表数据流向和受控主机所在的域。
受控地址范围	设置受控数据包发出的源地址范围。
端口范围	设置受控数据包发出的端口范围。
协议类型	设置受控数据包的协议类型。
带宽模式	独立模式即受控地址范围内每一个 IP 地址都将应用当前规则所设置的带宽限制；共享模式即受控地址范围内所有 IP 地址带宽总和为当前规则所设置的带宽限制。
上行最小保证带宽	设置上行最小保证带宽，即在物理带宽不足的前提下，上行数据流至少能够享有的最小带宽。
上行最大限制带宽	设置上行最大限制带宽，即上行数据流所能享有的最大带宽
下行最小保证带宽	设置下行最小保证带宽，即在物理带宽不足的前提下，下行数据流至少能够享有的最小带宽。
下行最大限制带宽	设置下行最大限制带宽，即下行数据流所能享有的最大带宽
规则生效时间表	设置规则的生效时间。
备注	添加对本条规则的说明信息。
启用/禁用规则	选择启用或禁用本条带宽控制规则。

- 规则列表

在规则列表中，可以对已保存的带宽控制规则进行相应设置。

图 4-35序号 1 规则的含义：与LAN口连接的IP地址为 192.168.1.2 - 192.168.1.254 范围的主机共享带宽，当这些主机通过路由器 1-65535 端口向WAN1 口发送所有协议格式的数据包，保证上行和下行的最小带宽各为 5000Kbps，最大带宽各为 10000Kbps。

说明：

- 单条规则生效的前提是：这条带宽控制规则所属接口的物理带宽足够大，且尚未被用尽。
- 异常情况：各带宽控制规则的最小保证带宽之和大于总物理带宽。当某接口所有带宽控制规则的最小保证带宽之和大于此接口的物理带宽时，意味着无论如何都无法同时满足所有带宽控制规则的最小保证带宽。
- 在 DMZ 口关闭状态下，不提供与 DMZ 口相关规则的新增、修改、启用或禁用操作，仅提供对该规则的删除操作。
- 只有当 DMZ 口开启时，DMZ 选项才在数据流向下拉菜单中显示。

4.6.1.3 游戏加速

游戏加速可优化游戏的速度体验，提高路由器通信即时、高效的特性。

界面进入方法：传输控制 >> 带宽控制 >> 游戏加速

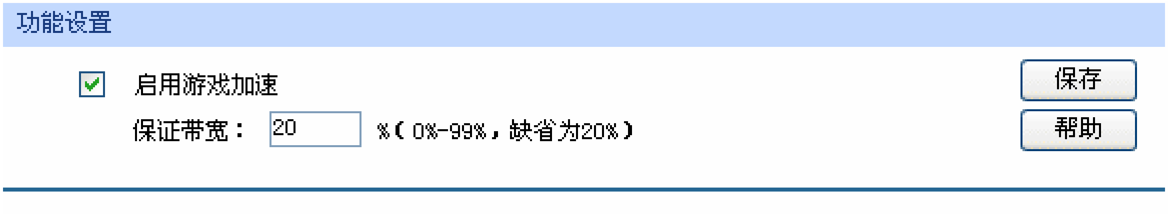


图 4-36 游戏加速设置界面

界面项说明：

➢ **功能设置**

启用游戏加速	勾选此项以启用游戏加速。不勾选时，设置不生效。
保证带宽	设置百分比数值，保证带宽将以数据流向上最小带宽的百分比生效。

4.6.2 连接数限制

作为局域网的统一出口，路由器支持的 TCP 和 UDP 连接数是有限的，如果局域网内有部分主机向广域网发起的 TCP 和 UDP 数目过多，影响局域网其他计算机的通信质量，就有必要对这部分计算机进行连接数限制。

4.6.2.1 连接数限制规则

可以在此对指定 IP 的计算机连接数限制进行设置。

界面进入方法：传输控制 >> 连接数限制 >> 连接数限制规则



图 4-37 连接数限制规则设置界面

界面项说明：

➢ 功能设置

启用连接数限制　　勾选此项以启用连接数控制。不勾选时，所有连接数限制均不生效。

➢ 连接数限制规则

IP 地址段　　设置需要进行连接数限制的主机的 IP 地址段。

最大连接数　　为本条规则设置相应的最大连接数。

备注　　添加对本条规则的说明信息。

启用/禁用规则　　选择启用或禁用本条规则。

➢ 规则列表

在规则列表中，可以对已保存的连接数限制规则进行相应设置。

图 4-37序号 1 规则的含义：IP地址为 192.168.1.101 的主机向广域网发起的最大连接数被限制为 100 条，该条规则已启用。

4.6.2.2 连接数监控

监控列表显示局域网主机的连接数限制情况。

界面进入方法：传输控制 >> 连接数限制 >> 连接数监控



监控列表

序号	IP地址	最大连接数	当前连接数
1	192.168.1.101	100	78
2	192.168.1.102	200	125
3	192.168.1.103	300	111
4	192.168.1.104	400	222
5	192.168.1.105	500	56

图 4-38 连接数监控界面

可通过监控列表搜索、查询局域网主机的连接数限制情况。如需获取最新局域网主机的连接数限制情况，请点击<刷新>按钮。

可通过监控列表搜索、查询局域网主机的连接数限制情况。如需获取最新局域网主机的连接数限制情况，请点击<刷新>按钮。

4.7 流量均衡

合理设置流量均衡，可以使路由器在多 WAN 口模式下更安全、有效地收发数据。

4.7.1 综合设置

界面进入方法：流量均衡 >> 综合设置

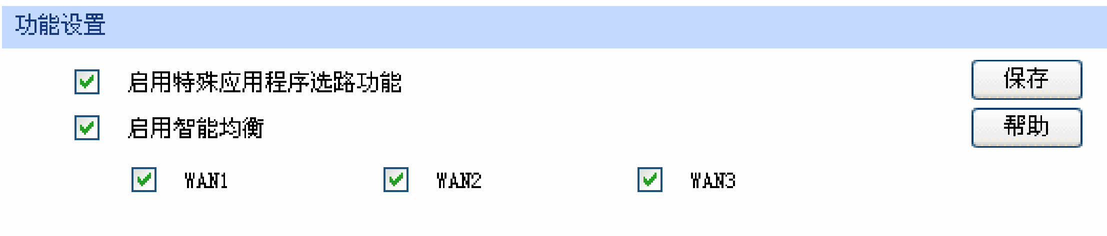


图 4-39 综合设置界面

勾选“启用特殊应用程序选路功能”，路由器会将数据包的源 IP 地址与目的 IP 地址作为一个整体，记录其通过的 WAN 口信息。后续如果有同一源 IP 地址和目的 IP 地址的数据包通过，则优先转发至上次记录的 WAN 口。该功能主要用于保证多连接应用程序的正常工作。

勾选“启用智能均衡”，并在下方选定 WAN 口，在没有任何选路规则的情况下，指定 WAN 口将自动进行流量均衡。

设置完成后点击<保存>按钮生效。

注意：

在实际应用中，如果某些 WAN 口没有连接到因特网，那么这些 WAN 口将不会参与智能均衡，请勿勾选。

4.7.2 策略选路

在此可以通过指定协议、地址范围、端口、WAN 口、生效时间，更精确地控制路由选路。

界面进入方法：流量均衡 >> 策略选路



图 4-40 策略选路设置界面

界面项说明：

➢ 选路规则设置

协议类型 在下拉列表中选择本条规则所针对的协议类型，不属于指定范围内的协议将不会应用选路规则。如果列表中没有您想指定的协议类型，可以参见**4.7.5 协议类型**进行添加，您可通过下拉列表旁边的<协议类型>按钮快速进入设置界面。

源地址范围 输入需要应用选路规则的源地址范围。输入 0.0.0.0 - 0.0.0.0 时表示匹配所有 IP。

目的地址范围 输入需要应用选路规则的目的地址范围。输入 0.0.0.0 - 0.0.0.0 时表示匹配所有 IP。

源端口范围 输入需要应用选路规则的源端口范围。只有当协议类型为 TCP、UDP、TCP/UDP 时可以指定范围，默认为 1 - 65535，表示匹配所有端口。

目的端口范围 输入需要应用选路规则的目的端口范围。只有当协议类型为 TCP、UDP、TCP/UDP 时可以指定范围，默认为 1 - 65535，表示匹配所有端口。

WAN 接口 在所列 WAN 口选项中选择数据流通过的 WAN 口。

规则生效时间表	指定规则生效时间，其他时间规则不生效。时间以 24 小时制进行设定，精确到分钟，下方可勾选生效的日期，以一周为单位。
启用/禁用规则	选择启用或禁用本条策略选路规则。

➢ 规则列表

在规则列表中，您可以对已保存的选路规则进行相应设置。

图 4-40序号 1 规则的含义：路由器收到源地址在 192.168.1.100 - 192.168.1.199 范围内，且发往目的地址在 116.30.10.1 - 116.30.1.20 范围内的数据包，不论端口与协议，全部从WAN1 接口进行转发，该规则已启用，永久生效。

4.7.3 ISP选路

通过 ISP 选路功能，可以将数据包转发至对应的 ISP 线路上，从而减少数据包在网络中被转发的次数，提高网络性能。

界面进入方法：流量均衡 >> ISP 选路

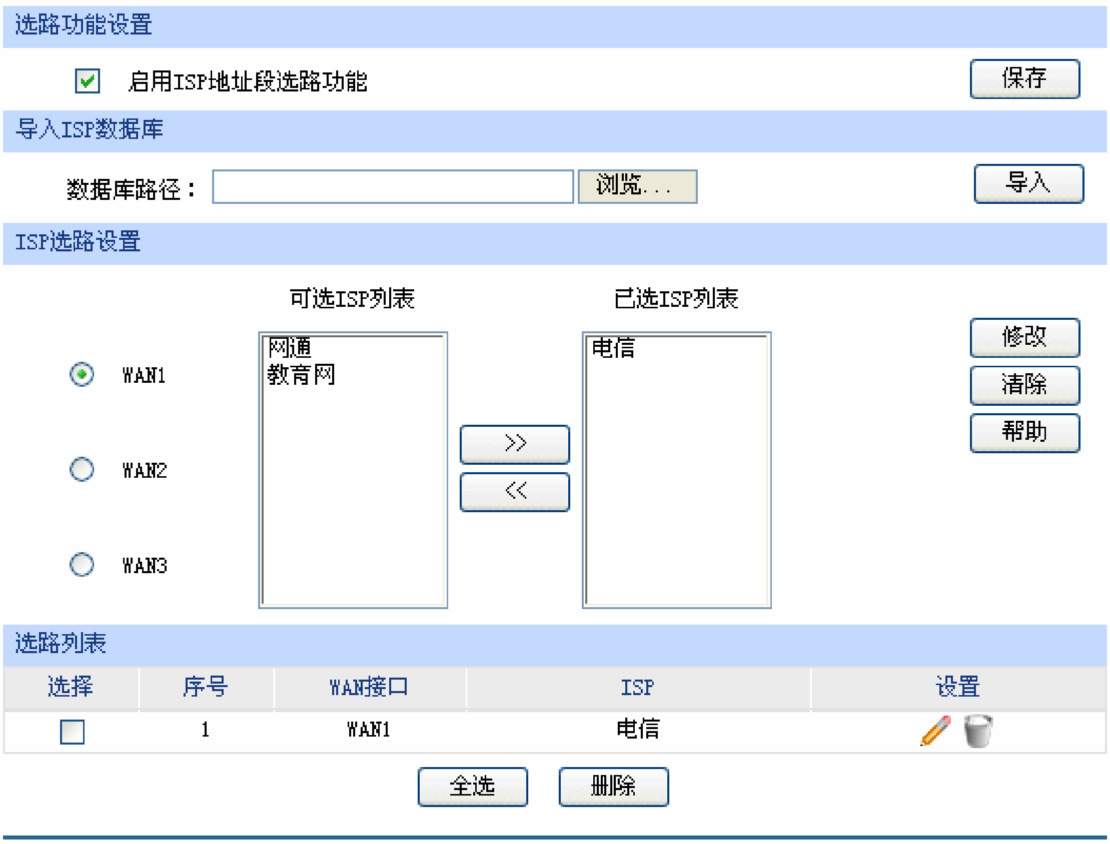


图 4-41 ISP 选路设置界面

界面项说明：

➢ 选路功能设置

勾选“启用 ISP 地址段选路功能”，点击<保存>按钮，下方的选路设置才能生效。

➢ **导入 ISP 数据库**

ISP 数据库即各 ISP 所拥有的 IP 地址段的数据库，通过匹配数据包目的 IP 地址与 ISP 数据库，路由器会将数据包从相应 ISP 所对应的 WAN 口转发。您可以在我司官方网站（http://www.tp-link.com.cn）上下载 ISP 数据库。

➢ **ISP 选路设置**

可选 ISP 列表	系统定义的 ISP 列表。选中合适的 ISP，点击< >> >按钮将其移至“已选 ISP 列表”中，一个 WAN 口可以选择多个 ISP。如果某 WAN 口对应的 ISP 不在可选列表中，则不需要设置该 WAN 口的 ISP 选路。
已选 ISP 列表	显示已经选择的 ISP。如果需要删除某个已选 ISP，请选中后点击< << >按钮将其移回“可选 ISP 列表”。

➢ **选路列表**

在选路列表中，您可以对已保存的 ISP 选路进行相应设置。

图 4-41序号 1 规则的含义：WAN1 接口对应电信ISP，所有从WAN1 转发的数据包将通过电信线路进入广域网。

注意：

智能均衡、策略选路、ISP 选路三个功能可以同时工作，但当三个功能设置有冲突时，路由器执行的优先顺序为：策略选路 > ISP 选路 > 智能均衡。

4.7.4 线路备份

路由器默认所有 WAN 口都处于自动备份模式，当有 WAN 口发生故障时，其流量会均衡到其他 WAN 口上，当故障 WAN 口恢复后系统会再次均衡所有 WAN 口的流量。

根据实际需要合理设置线路备份，可以减轻 WAN 口流量负担，提高网络效率。

界面进入方法：流量均衡 >> 线路备份



图 4-42 备份配置界面

界面项说明：

➢ 备份配置

WAN 口列表 显示当前路由器所有正在工作的 WAN 口，可以拖动浅蓝色的 WAN 口图标，将其添加至下方的主 WAN 组或备 WAN 组中，若 WAN 口图标变为灰色，则表示该 WAN 口已经存在主备关系。

主备组设置 备 WAN 组中的 WAN 口将在指定条件下分担主 WAN 组中 WAN 口的流量。主 WAN 组可以包含一个或多个 WAN 口，备 WAN 组只能指定一个 WAN 口。

备份模式 可以选择定时备份或故障备份。选择定时备份时，下方可进行备份生效时间设置；选择故障备份时，下方可进行故障备份设置。

备份生效时间 指定备份生效时间，在生效时间内启动备份 WAN 口，关闭主 WAN 口。时间以 24 小时制进行设定，精确到分钟，下方可勾选生效的日期，以一周为单位。如果不勾选星期，则生效时间以一天为单位，若开始时间大于结束时间，则默认时间跨度是从当天到次日。

故障备份 指定故障备份条件。在主 WAN 口正常工作时备份 WAN 口不工作，只有当符合故障备份条件时才会启动备份 WAN 口。

启用/禁用规则	选择启用或禁用本条主备配置规则。

➢ 主备组列表

在主备组列表中，您可以对已保存的主备规则进行相应设置。

图 4-42序号 1 规则的含义：WAN1 口与WAN2 口为主备关系，当WAN1 口发生故障时启用WAN2 口，该规则已启用。

注意：

主 WAN 组和备 WAN 组中不能放置相同的 WAN 口，且一个 WAN 口只能置入一个主备组中。

4.7.5 协议类型

为了让您能够在定制选路策略时比较方便地指定应用选路规则的协议，设备提供了协议类型管理功能。每一个协议类型由协议名称和协议号两部分构成。系统已经预定义了 TCP、UDP、TCP/UDP 三种常用协议类型，您也可以根据需要添加自定义协议类型。

界面进入方法：流量均衡 >> 协议类型



图 4-43 协议类型设置界面

界面项说明：

➢ 协议类型

协议名称	用户自定义，标识一条协议类型。该名称将显示在“访问规则”设置的服务类型下拉列表中。
协议号	IP 数据包中协议字段的内容，取值范围为 0 - 255。

➢ 协议列表

在协议列表中，您可以对自定义的协议类型条目进行相应设置。

注意：

系统预定义的协议类型不可进行配置操作。

4.8 路由设置

4.8.1 静态路由

路由，是选择一条最佳路径把数据从源地点传送到目的地点的行为。静态路由则是由网络管理员手动配置的一种特殊路由，具有简单、高效、可靠等优点。

静态路由不随着网络拓扑的改变而自动变化，多用于网络规模较小，拓扑结构固定的网络中。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手动修改路由表中相关的静态路由信息。

界面进入方法：路由设置 >> 静态路由



图 4-44 静态路由表设置界面

界面项说明：

➢ 静态路由规则

目的地址	设定数据报包需要到达的目的 IP 地址。
子网掩码	设定目的 IP 地址的子网掩码。
下一跳	指定一个 IP 地址，路由器下一步会将符合条件的数据包转发到该地址上。

出接口	设定数据包发送出去的接口。
备注	添加对本条规则的说明信息。

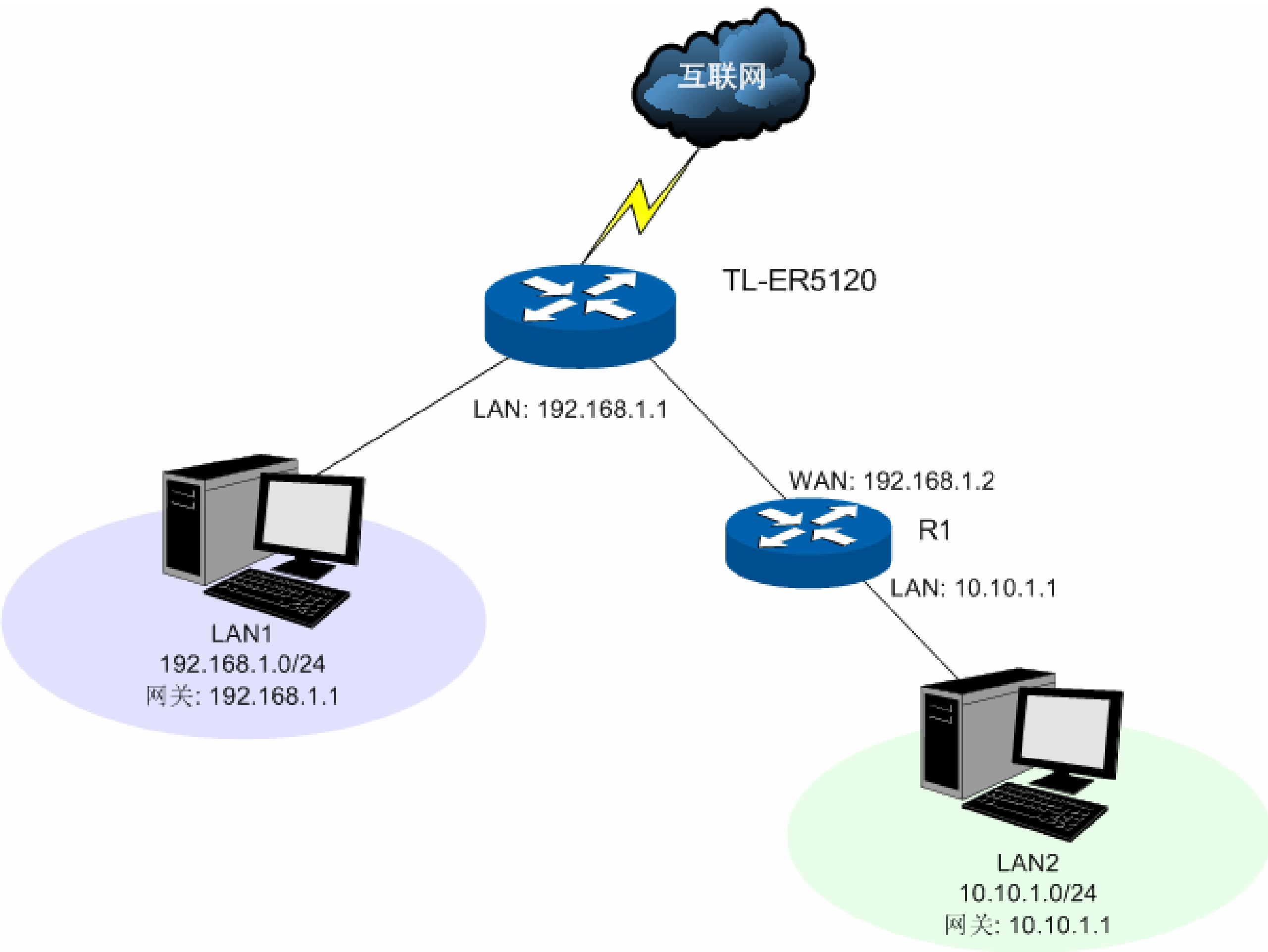
➢ 规则列表

在规则列表中，可以对已保存的静态路由规则进行相应设置。

序号 1 规则的含义：如果有数据包从 LAN 口发往一个 IP 地址为 192.168.3.56，子网掩码为 255.255.255.255 的设备，则路由器会将数据包转发至下一跳地址 192.168.3.1，该路由规则已启用。

应用举例

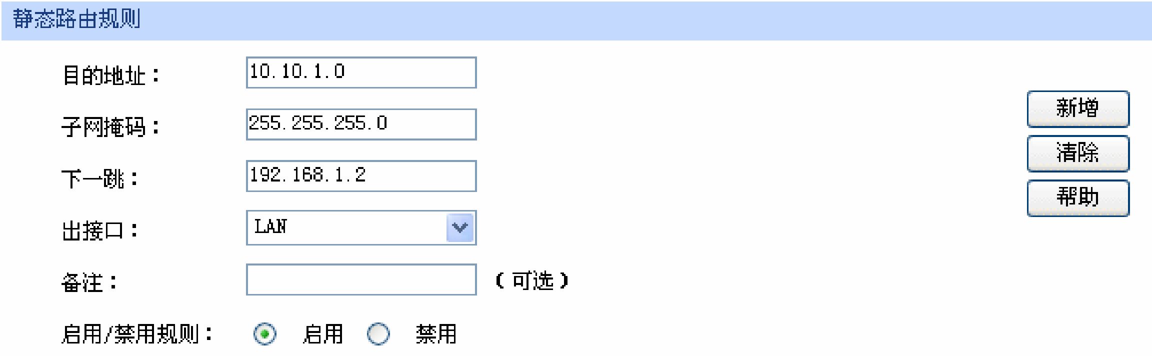
某网吧的网络结构如下：



TL-ER5120 的 LAN 口连接 LAN1（192.168.1.0/24 网段），同时级联另一路由器，该路由器连接 LAN2（10.10.1.0/24 网段），现在要实现 LAN1 中的主机能访问 LAN2。

可以通过设置一条静态路由来实现。首先，设置路由器 R1 的 LAN 口 IP 地址为 10.10.1.1，WAN 口 IP 地址为 192.168.1.2，同时设置其网关地址为 TL-ER5120 的 LAN 口 IP 地址 192.168.1.1。

在 TL-ER5120 静态路由界面设置到 10.10.1.0/24 网段的下一跳地址为路由器 R1 的 WAN 口地址 192.168.1.2，如下图。最后点击<新增>按钮保存规则。



4.8.2 RIP服务

RIP（Routing Information Protocol，路由信息协议），是一种采用距离向量算法选择最优路径的动态路由协议，因其易于配置、管理和实现，被广泛应用于如校园网等中小规模的网络中。

RIP 的距离是数据包发往目的站点需经过的路由跳数，取值为 1 - 15，超过 15 则是无穷大，表示目的地无法到达。最优路径即所经跳数最少的网络链路。RIP 每隔 30 秒通过 UDP 报文以广播形式交换一次路由信息。如果某一路由在 180 秒内未发送路由信息，则其他路由上的 RIP 协议就会将到该路由的距离设定成无穷大，并删除路由表中相关信息。

RIP 协议在应用中不断地被完善，从最初的 RIPv1 版本基础上逐渐发展出了 RIPv2 版本的协议。RIPv2 相较 RIPv1 还支持 VLSM(Variable Length Subnet Mask，可变长子网掩码)、简单明文认证、MD5 密文认证、CIDR（Classless Inter-Domain Routing，无类型域间选路）和多播，相对于 RIPv1 应用更加灵活。

TL-ER5120 同时支持 RIPv1 和 RIPv2 两种版本的协议，可以根据实际的网络需求设置，以提高网络性能。

界面进入方法：路由设置 **>> RIP** 服务



图 4-45 RIP 服务设置界面

界面项说明：

- **RIP 服务设置**

接口	显示目前路由器所有存在物理连接或是已经分配静态 IP 的接口。
接口状态	选择是否启用 RIP 协议。
输出版本	选择是以何种形式向外发送路由信息。其中 RIPv2 支持多播和广播两种形式。
密码认证	如果应用 RIPv2，可以根据实际网络情况设置密码认证，认证密码不超过 15 位。
所有接口	在此可以对所有接口进行批量操作。接口状态增加“禁用”一项，选择后所有接口都不应用 RIP 协议。

- **RIP 路由表**

启用 RIP 协议后，路由器收到数据包后经 RIP 协议转发的信息将会显示在列表中。

图 4-45序号 1 条目的含义：当收到目的地址在 116.20.10.0/24 网段的数据包时，路由器将选择与目的地址同网段的WAN1 口作为下一跳，并转发数据，此时下一跳IP地址为 116.20.10.116.。数据包经过的跳数为 1，该条目的生存时间为 0 秒，表示永久生效。

注意：

- 当系统模式为 NAT 模式时不支持 RIP 路由设置，若需设置 RIP 路由，请更改当前系统模式。
- 仅当 WAN 口的连接方式为静态 IP 时，该 WAN 口的 RIP 服务才会生效。

4.9 端口设置

TL-ER5120 路由器具备一些简单的交换机端口管理功能。在此可以实时查看路由器各端口的数据流通状况，并进行相应的控制和管理。

4.9.1 端口统计

用于交换信息的数据包在数据链路层通常称为“帧”。可以通过此功能查看各个端口收发数据帧的统计信息。

界面进入方法：端口设置 >> 端口统计

统计列表

参数		端口1	端口2	端口3	端口4	端口5
接收	单播帧	104998	0	0	64607	0
	广播帧	27805	0	0	84	0
	流控帧	0	0	0	0	0
	多播帧	7238	0	0	37	0
	所有帧	131581297	0	0	9997674	0
	过小帧	0	0	0	0	0
	正常帧	140041	0	0	64728	0
	过大帧	0	0	0	0	0
发送	单播帧	62536	0	0	112970	0
	广播帧	1	0	0	10	0
	流控帧	0	0	0	0	0
	多播帧	0	0	0	2	0
	所有帧	15364631	0	0	139504476	0
	清空统计	☐	☐	☐	☐	☐

刷新 清空所有 帮助

图 4-46 端口统计界面

界面项说明：

➢ 统计列表

单播帧 目的 MAC 地址为单播 MAC 地址的正常数据帧数目。

广播帧 目的 MAC 地址为广播 MAC 地址的正常数据帧数目。

流控帧 接收/发送的流量控制数据帧数目。

多播帧 目的 MAC 地址为多播 MAC 地址的正常数据帧数目。

所有帧 接收/发送所有的数据帧的总字节数（包含校验和错误的帧）。

过小帧 收到的长度小于 64 字节的数据帧数目（包含校验和错误的帧）。

正常帧 收到的长度在 64 字节到最大帧长之间的数据帧数目（包含错误帧）。对于不带 tag 标签的帧，路由器支持的最大帧长为 1518 字节；对于带 tag 标签的帧，路由器支持的最大帧长为 1522 字节。

过大帧 收到的长度大于最大帧长的数据帧数目（包含错误帧）。

勾选最后一行的复选框后，点击<清空统计>按钮，即可清空该列对应端口的统计数据。点击<清空所有>按钮可以一次清空所有统计数据。

4.9.2 端口监控

可以在此开启和设置端口监控功能。被监控端口的报文会被自动复制到监控端口，以便网络管理人员实时查看被监控端口传输状况的详细资料，对其进行流量监控、性能分析和故障诊断。

界面进入方法：端口设置 >> 端口监控



图 4-47 端口监控设置界面

界面项说明：

➢ 功能设置

启用端口监控	勾选即启用端口监控。推荐勾选，方便及时了解路由器端口报文信息。
监控模式	选择对数据包进行“输出监控”或者“输入输出监控”。

➢ 监控列表

监控端口	只能选择一个端口做监控端口。
被监控端口	被监控端口可以为多个，但不包含当前的监控端口。

图 4-47监控列表的含义是：端口 4 被选作监控端口，它将对端口 1、2、3、5 进行输出监控。

说明

如果监控端口为 LAN 口，被监控端口中有其他 LAN 口，则这些 LAN 口必须属于同一个 Port VLAN。比如端口 3 和端口 4 都设置成 LAN 口，端口 3 为监控端口，端口 4 为被监控端口，那么端口 3 和端口 4 必须处于相同的 Port VLAN 中，端口监控功能才能生效。

应用举例

某网吧网络出现异常状况，需要利用端口监控功能捕获网络中的所有数据进行分析。

可通过端口监控实现此需求。勾选“启用端口监控”，并选择“输入输出监控”的监控模式，设置端口 3 为监控端口，监控其它端口的输入输出数据，如下图。设置完成后，点击<保存>按钮。



4.9.3 端口流量限制

可以在此开启各端口的流量限制功能并进行相应设置。

界面进入方法：端口设置 >> 端口流量限制



图 4-48 端口流量限制设置界面

界面项说明：

➢ 功能设置

端口　　显示所有物理端口，需要对某个端口进行流量限制时，在其对应行设置即可。

入口限制状态　　勾选“启用”后，后续设置的入口限制模式和速率才会生效。

入口限制模式　　有“所有帧”、“FLOOD”（端口的广播、多播帧以及目的 MAC 地址不存在于地址表的帧）、“广播和多播”和“广播”四种模式，选择其一。

入口限制速率　　有从小到大 128Kbps/ 256Kbps/ 512Kbps/ 1Mbps/ 2Mbps/ 4Mbps/ 8Mbps 七种速率，选择其一。

出口限制状态　　勾选“启用”，后续设置的出口限制速率才会生效。

出口限制速率　　有从小到大 128Kbps/ 256Kbps/ 512Kbps/ 1Mbps/ 2Mbps/ 4Mbps/ 8Mbps 七种速率，选择其一。

图 4-48第一行的含义是：开启端口 1 的入口和出口限制状态，设置端口 1 的入口限制模式为FLOOD，并将其入口/出口速率均设为 256Kbps。设置完成后，端口 1 的FLOOD模式入口数据帧的接收速率及所有出口数据帧的发送速率将不会超过 256Kbps。

4.9.4　端口参数

可以在此启用各物理端口及其流量限制，并根据需要设定其协商模式。

界面进入方法：端口设置 >> 端口参数



图 4-49 端口参数设置界面

界面项说明：

➢ 功能设置

端口状态　　只有勾选了“启用”该端口才会有数据包的传输，即物理意义上的开启。

流量控制　　推荐勾选“启用”以控制调节各端口数据包转发的速率，避免出现拥塞。

协商模式　　有 10M 全/半双工、100M 全/半双工、自协商 5 种模式可选，择需使用。

所有端口　　　　　这一栏可对以上所有端口进行统一设置，比如同时启用或禁用。

4.9.5 端口状态

可以在此查看各个端口的基本状态。

界面进入方法：端口设置 >> 端口状态

状态列表

端口	端口状态	连接速率(Mbps)	双工模式	流量控制
1	已连接	100	全双工	启用
2	未连接	---	---	---
3	未连接	---	---	---
4	已连接	100	全双工	启用
5	未连接	---	---	---

刷新　帮助

图 4-50 端口状态界面

4.9.6 Port VLAN

VLAN(Virtual Local Area Network，虚拟局域网)是从逻辑上而非物理上，将整个局域网分割成几个不同的广播域，数据只能在 VLAN 内进行交换。

一个稍具规模的网络如果只有一个广播域，那么在网络内不断发送的广播包很容易造成广播风暴，消耗网络整体带宽，并给网络中的主机带来额外的负担。划分 VLAN 以后，数据只会在自己所属的 VLAN 内广播，所以可以控制广播风暴，同时还能增强网络安全，简化网络管理。

TL-ER5120 提供基于端口划分 VLAN 的 Port VLAN 功能，可以把路由器的若干 LAN 口从逻辑上划分为多个 VLAN。

界面进入方法：端口设置 >> Port VLAN

功能设置

参数	端口1	端口2	端口3	端口4	端口5
网络	WAN	WAN	WAN	LAN	DMZ
VLAN	VLAN7	VLAN8	VLAN9	VLAN1	VLAN5

保存　帮助

图 4-51 Port VLAN 设置界面

界面项说明：

➢ 功能设置

网络 标识各个物理端口此时属于的逻辑网络。

VLAN 配置各端口所属 VLAN。

说明

- Port VLAN 的划分只能在 LAN 口中进行。
- 当 DMZ 接口的状态改变的时候，会影响到原先 Port VLAN 的配置。当改变 DMZ 接口的状态后，建议检查 Port VLAN 的配置，必要时重新设置。

4.10 系统服务

可在此便捷地应用 UPnP、DDNS 服务，并可通过 Web 服务器功能实现远程管理路由器。

4.10.1 UPnP服务

UPnP(Universal Plug and Play, 通用即插即用)协议，遵循此协议的不同厂商的各种设备可以自动发现对方并进行连接。

如果应用程序支持 UPnP 协议，而局域网中的主机安装了 UPnP 组件，路由器开启了 UPnP 服务后，局域网中的主机就可以根据软件的需要自动地在路由器上打开相应的端口，使得外部主机上的应用程序在需要时能够通过打开的端口访问内部主机上的资源，这样原本受限于 NAT 的功能便可以正常使用。例如，Windows XP 和 Windows ME 系统上安装的 MSN Messenger，在使用音频和视频通话时就可以利用 UPnP 协议。

相对于转发规则而言，UPnP 的应用不需要用户手动设置任何规则，对于一些端口不固定的应用会更加方便。

界面进入方法：系统服务 **>> UPnP** 服务 **>> UPnP** 服务

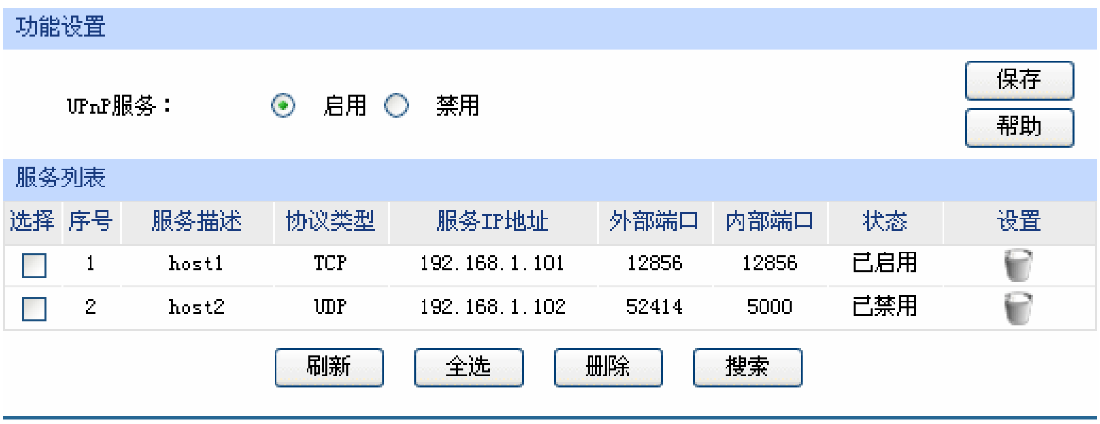


图 4-52 UPnP 服务设置界面

界面项说明：

➢ 功能设置

UPnP 服务　　　　选择启用或禁用 UPnP 服务。

➢ 服务列表

启用 UPnP 后，所有应用到 UPnP 的连接规则会显示在服务列表中，TL-ER5120 可以同时支持 64 条 UPnP 服务，并对已有规则进行相应设置。

图 4-52序号 1 条目的含义：在路由器WAN口的 12856 端口接收到的TCP数据，将转发到局域网服务器 192.168.1.101 的 12856 端口上。

注意：

- 应用时不仅要在路由器上启用 UPnP 服务，还需要确认主机操作系统和应用程序也支持此服务，即 Windows XP 系统需安装 UPnP 组件；应用程序本身需支持 UPnP，如 MSN 最新版、电驴、迅雷等。
- 一些木马、病毒可能会利用 UPnP 服务打开特定的端口，使局域网主机成为黑客的攻击目标，因此需谨慎应用 UPnP 服务。

4.10.2 动态DNS

4.10.2.1 花生壳动态域名

广域网中，许多 ISP 使用 DHCP 分配公共 IP 地址，因此用户端获得的公网 IP 是不固定的。当其它用户需要访问此类 IP 动态变化的用户端时，很难实时获取它的最新 IP 地址。

DDNS(Dynamic DNS,动态域名解析服务)服务器则为此类用户端提供了一个固定的域名，并将其与用户端最新的 IP 地址进行关联。当服务运行时，DDNS 用户端把最新的 IP 地址通知 DDNS 服务器，服务器会更新 DNS 数据库中域名与 IP 的映射关系。而对于访问它的用户端，将会得到正确的 IP 地址并成功访问服务端。DDNS 常用于 Web 服务器搭建个人网站、FTP 服务器提供文件共享等，访问的用户可以便捷地获取服务。

路由器作为动态 DNS 客户端，本身并不提供动态 DNS 服务。因此，在使用此功能之前，必须进入动态 DNS 服务提供商的官方主页注册，以获得用户名、密码和域名等信息。TL-ER5120 路由器提供花生壳动态 DNS 客户端。

界面进入方法：系统服务 >> 动态 DNS >> 花生壳动态域名



图 4-53 花生壳动态域名设置界面

界面项说明：

➢ 功能设置

用户名	填入在花生壳网站注册的用户名。若还没有注册，请点击右边的链接“注册用户名”登录花生壳网站进行注册。
密码	填入在花生壳网站注册该用户名时所设置的密码。
服务开关	选择启用或禁用花生壳动态域名服务。
接口名	显示启用花生壳动态域名服务的 WAN 口。
服务类型	服务启用之后，显示当前登录的 DDNS 账号是属于专业服务还是标准服务。这取决于您在注册时选择的服务类型。
连接状态	显示 DDNS 的工作状态。 “服务没有运行”表示 DDNS 功能未启用； “服务连接中，请等候”表示系统正在连接 DDNS 服务器； “服务已运行”表示 DDNS 工作正常； “用户名或密码错误”表示输入的用户名或密码有误，请重新输入正确的值后再启用 DDNS。
域名信息	显示当前登录的 DDNS 用户所拥有的域名。用户可以申请多个域名，点击“查看所有域名”显示当前用户申请的所有域名，但最多显示 16 条。

➢ 管理列表

在管理列表中，可以对当前的 DDNS 条目进行相应设置。

图 4-53条目 1 的含义：应用于WAN1 口的花生壳用户名是uername1，对应的域名是user1.oray.net，该服务已运行。

4.10.3 Web服务器

TL-ER5120 内置 Web 服务器，您可以非常方便地通过 Web 浏览器登录 TL-ER5120 的 Web 管理界面。即使在外部网络，同样也可以登录 Web 界面管理路由器。这只需要在 Web 服务器界面设置一些相关参数：访问路由器的用户名密码、允许远端登录的 IP 地址范围以及服务端口等。

4.10.3.1 用户设置

在此可以修改登录时使用的用户名和密码。

界面进入方法：系统服务 >> Web 服务器 >> 用户设置

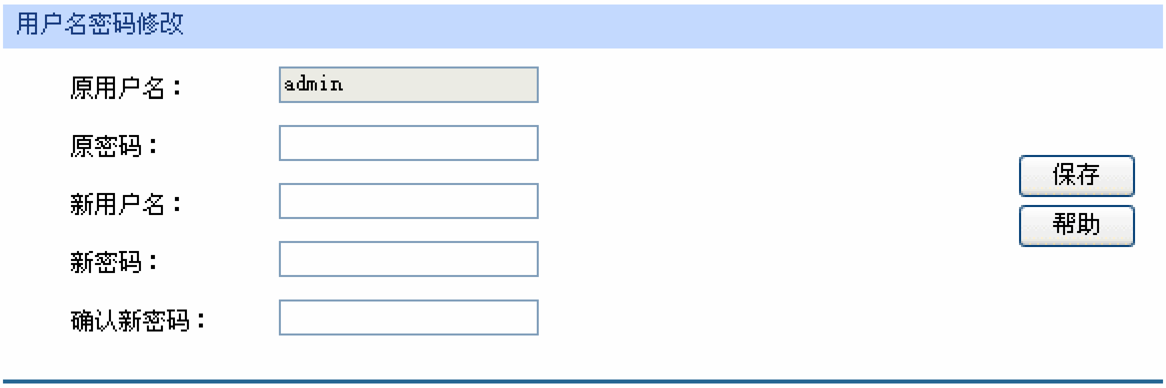


图 4-54 用户设置界面

界面项说明：

➢ 用户名密码修改

原用户名	本次登录路由器的用户名。
原密码	本次登录路由器使用的密码。
新用户名	重新设置登录路由器的用户名。
新密码	重新设置登录路由器的密码。
确认新密码	再次输入新密码。

说明

出厂的用户名/密码是 admin/admin。更改用户名密码并保存生效后，后续登录时请使用新用户名及密码。用户名和密码最大支持 31 个字符，且只能是数字和字母，区分大小写。

4.10.3.2 远程管理

可以在远程管理界面对允许远程登录的 IP 地址范围进行设置和修改。

界面进入方法：系统服务 **>> Web** 服务器 **>>** 远程管理



图 4-55 远程管理设置界面

界面项说明：

➢ 远程管理地址

远程地址范围	设置需要从外部网络登录路由器的主机地址，可指定单个 IP 或一个网段。
启用/禁用规则	选择启用或禁用该规则。

➢ 地址列表

在地址列表中，可以对已保存的远程管理地址条目进行相应设置。

图 4-55序号 1 条目的含义：允许IP地址属于 172.31.70.0/24 网段的主机登录路由器Web界面，该规则已启用。

4.10.3.3 服务设置

可以在服务端口界面对 Web、Telnet 服务的端口进行设置和修改。

界面进入方法：系统服务 **>> Web** 服务器 **>>** 服务端口

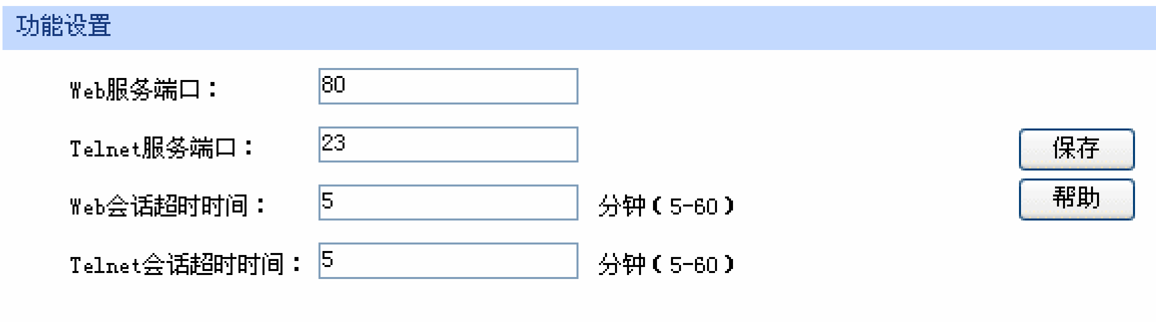


图 4-56 服务端口设置界面

界面项说明：

➢ 功能设置

Web 服务端口	设置路由器的 Web 服务端口。
Telnet 服务端口	设置路由器的 Telnet 服务端口。
Web 会话超时时间	设置通过 Web 页面访问路由器的超时时间，当用户登录 Web 界面后在设定时间内无任何操作将会自动丢失连接。
Telnet 会话超时时间	设置通过 Telnet 远程访问路由器的超时时间，当用户远程登录路由器后在设定时间内无任何指令将会自动丢失连接。

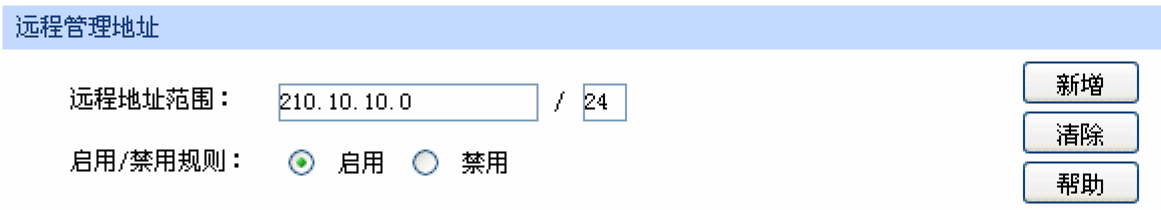
注意：

路由器默认的 Web 服务端口为 80。如果改为其它值，在局域网或广域网都必须用“http://IP 地址:端口”的方式才能登录路由器。例如，将 Web 管理端口更改为 88，在局域网内登录时的 URL 地址应为 **http://192.168.1.1:88**。

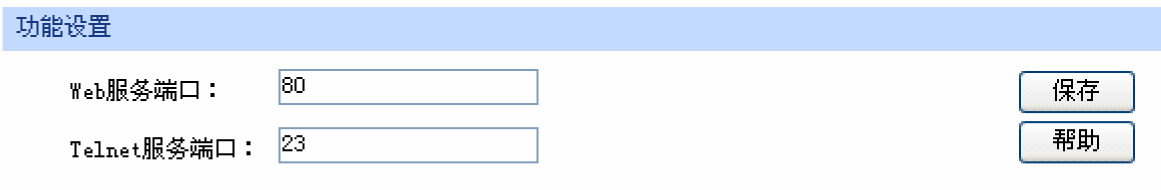
应用举例：

某网吧路由器地址为 210.10.10.50，为方便管理，希望广域网 210.10.10.0/24 网段的 IP 地址能对路由器进行远程管理。

可以通过设置 Web 服务器实现此需求。首先需要设置远端访问路由器的地址段，并选择启用该访问规则，如下图所示：



在服务端口界面为 Web 服务器开放相应的服务端口，设置如下图所示（以默认值为例）：



在浏览器地址栏输入路由器地址 210.10.10.50 登录路由器 Web 界面。

4.11 系统工具

系统工具可帮助您对路由器系统进行全局管理，以及测试网络连通性。

4.11.1 设备管理

4.11.1.1 恢复出厂配置

界面进入方法：系统工具 >> 设备管理 >> 恢复出厂配置

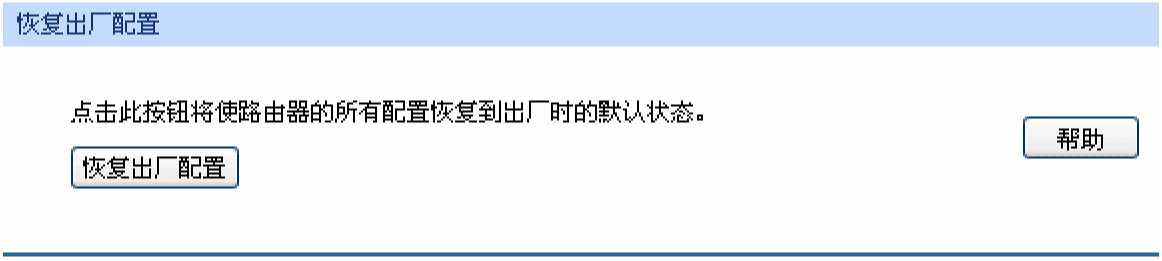


图 4-57 恢复出厂配置界面

点击<恢复出厂配置>按钮，路由器将会恢复所有设置的默认值。建议在网络配置错误、组网环境变更等情况时使用此功能。

4.11.1.2 备份与导入配置

界面进入方法：系统工具 >> 设备管理 >> 备份与导入配置

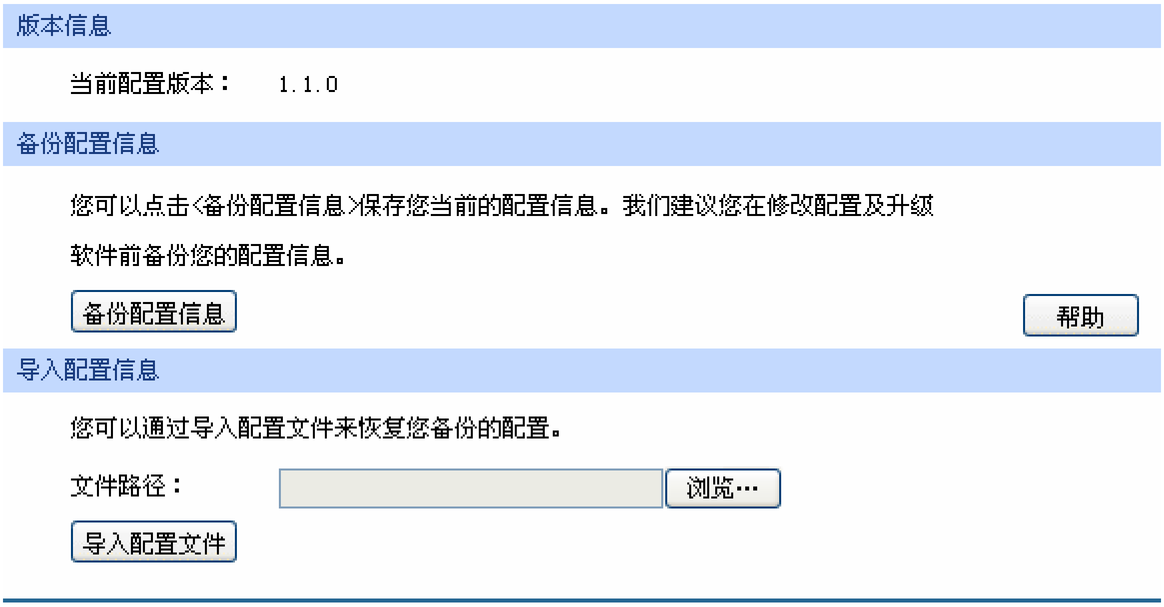


图 4-58 备份与导入配置界面

➢ 版本信息

显示当前路由器软件版本。

➢ 备份配置信息

单击<备份配置信息>按钮，路由器会将目前所有已保存配置导出为文件。建议在修改配置或升级软件前备份当前的配置信息。

➢ 导入配置信息

单击<浏览>按钮，选择已备份的配置文件；或者在文件路径输入框中填写完整的配置文件路径，然后点击<导入配置文件>按钮，将路由器恢复到以前备份的配置状态。

注意：

- 备份及导入文件过程中请保持电源稳定，避免强行断电。
- 导入的配置文件版本与路由器当前配置版本差距过大，将有可能导致路由器现有配置信息丢失，如果有重要的配置信息，请谨慎操作。

4.11.1.3 重启路由器

界面进入方法：系统工具 >> 设备管理 >> 重启路由器

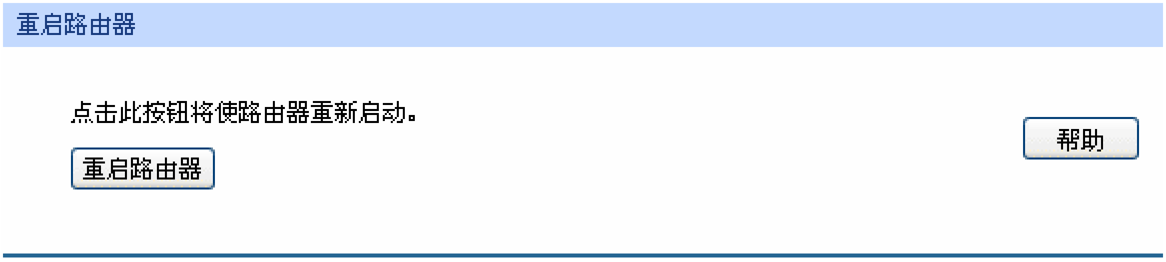


图 4-59 重启路由器界面

单击<重启路由器>按钮，路由器将会重新启动。

重新启动不会丢失已保存的配置，在重启的过程中，网络连接将会暂时中断。

注意：

路由器重启过程中请保证电源稳定，避免强行断电。

4.11.1.4 软件升级

界面进入方法：系统工具 >> 设备管理 >> 软件升级

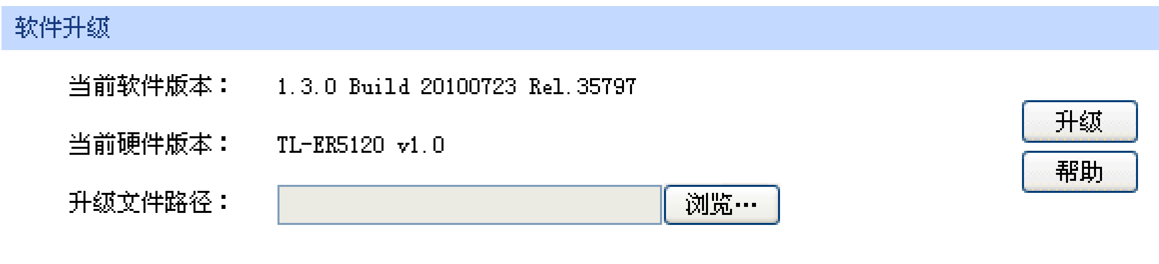


图 4-60 软件升级界面

TP-LINK 官方网站（http://www.tp-link.com.cn）会不定期更新 TL-ER5120 的软件升级文件，可将升级文件下载保存在本地。登录 TL-ER5120 路由器后进入软件升级界面，单击<浏览>按钮，选择保存路径下的升级文件，点击<升级>进行软件升级。

注意：

- 软件升级成功后路由器将会自动重启，在路由器重启完成前请保证电源稳定，避免强行断电。
- 软件升级后由于新旧版本软件的差异可能会恢复出厂默认配置，如有重要配置信息，请在升级前备份。

4.11.2 诊断工具

4.11.2.1 诊断工具

可在诊断工具界面通过 ping 命令或 tracert 命令来诊断当前路由器的网络连接状态。

界面进入方法：系统工具 >> 诊断工具 >> 诊断工具

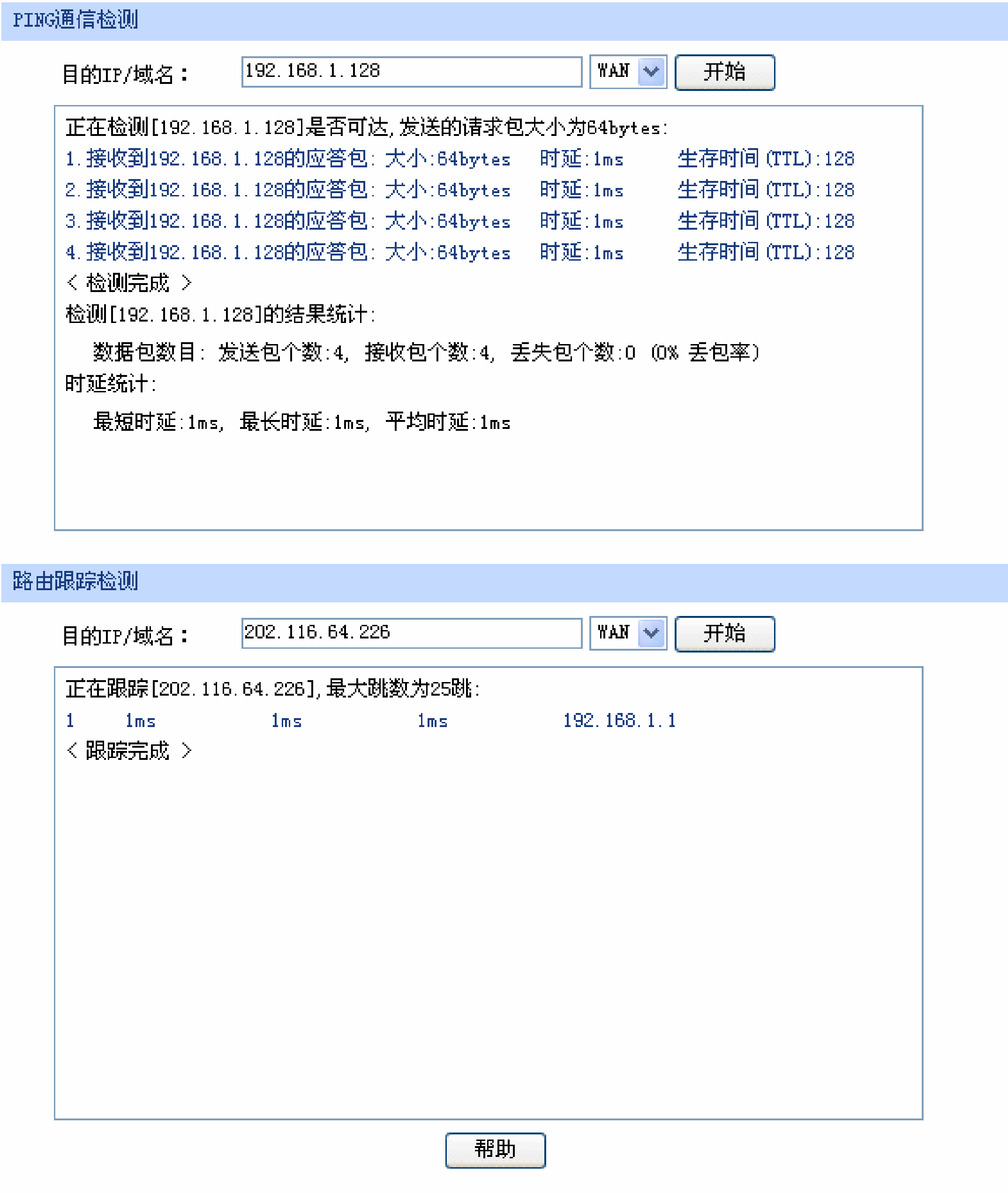


图 4-61 诊断工具界面

界面项说明：

➢ **Ping 通信检测**

目的 IP/域名	输入目的地址，可以是一个合法 IP 地址，也可以是一个合法域名，如果输入地址无效将提示重新输入。在下拉菜单中选择目的地址所属接口。点击<开始>按钮后，路由器将发送 ping 包检测目的地址是否可以达到，并在下面的方框中显示检测结果。

➢ 路由跟踪检测

目的 IP/域名	输入目的地址，可以是一个合法 IP 地址，也可以是一个合法域名，如果输入地址无效将提示重新输入。在下拉菜单中选择目的地址所属接口。点击<开始>按钮后，路由器将发送 tracert 包检测目的地址经过哪些路由到达，并在下面的方框中显示检测结果。

4.11.2.2 在线检测

该页面用于检测 WAN 口是否在线。

界面进入方法：系统工具 >> 诊断工具 >> 在线检测



界面项说明：

➢ 检测设置

接口名	选择需要在线检测的 WAN 口。
检测开关	选择开启或者关闭在线检测。关闭在线检测时，路由器只根据 WAN 接口的物理连接状态和拨号状态判断是否在线；开启在线检测时，路由器将综合 PING 检测和 DNS 检测的结果判断是否在线。

检测模式 选择自动在线检测或者手动在线检测。自动模式下，PING 检测选择网关作为目的地址，DNS 检测选择 WAN 口 DNS 服务器作为目的地址；手动模式下，您可以自己设置 PING 检测和 DNS 检测的目的地址。

PING 检测 在手动在线检测模式下，可以输入 PING 检测的目的 IP 地址。输入 0.0.0.0 表示不进行 PING 检测。

DNS 检测 在手动在线检测模式下，可以输入 DNS 服务器的 IP 地址。输入 0.0.0.0 表示不进行 DNS 检测。

➢ WAN 口状态列表

WAN 口 显示所检测的 WAN 口。

检测 显示选择的检测开关，即启用或禁用。

WAN 口状态 显示 PING 检测或 DNS 检测的结果。

4.11.3 流量统计

流量统计界面将显示接入路由器 LAN 口或 DMZ 口的局域网设备向广域网发出数据的流量统计。

界面进入方法：系统工具 **>>** 流量统计



图 4-62 流量统计界面

路由器默认勾选“启用流量统计”、“启用自动刷新”选项，启用自动刷新时，路由器每隔 5 秒刷新一次。在下拉菜单中选择流量统计接口类型后，相应的流量统计信息将显示在流量统计列表中。可以按照不同的表头对表格进行排序，默认排序方式为从小到大。

第5章 典型配置

5.1 典型配置需求

某网吧配置需求如下：

- 两条电信 10M 光纤接入，共有 150 台电脑，网吧分为普通区（100 台）和特殊区（50 台）。
- 需要防范局域网内的 ARP 攻击和 ARP 欺骗。
- 需要防范广域网的 ARP 攻击。
- 需要防范 DoS 攻击等常见网络攻击。
- 需要针对普通区和特殊区进行不同的带宽设置，给予不同的带宽享受，同时防止个别用户过度占用带宽而影响其它用户的正常上网。
- 需要保证游戏顺畅，满足网吧以游戏客户为主的客户群。
- 需要进行连接数限制，以防止某台电脑过度占用连接数影响其他电脑的正常上网。
- 需要保证公安局网络监控软件能够对所有局域网到广域网的信息进行监控。

5.2 典型配置方案

为满足上面的典型配置需求，使用 TP-LINK 多 WAN 口高性能网吧路由器 TL-ER5120 进行组网，以下面的具体组网方案为例进行说明：

- 电信光纤线路通过光纤收发器接入路由器，WAN 口接入方式采用静态 IP 接入方式；
- 禁用 ER 系列网吧路由器的 DHCP 服务器功能，手动给局域网内电脑分配静态 IP 地址；
- 使用 IP MAC 地址绑定功能，绑定局域网主机的 IP 与 MAC 信息，实现局域网 ARP 攻击防护；
- 开启发送免费 ARP 包功能，实现局域网 ARP 防欺骗功能；
- 使用 IP MAC 地址绑定功能，绑定 WAN 口网关的 IP 与 MAC 信息，实现广域网 ARP 攻击防护；
- 设置攻击防护功能，实现 DoS 类、扫描等攻击防护；
- 设置带宽控制条目，分配给普通区每台主机的最小保障带宽为 100kbps，最大限制带宽为 800Kbps；分配给特殊区每台主机的最小保障带宽为 100kbps，最大限制带宽为 1000Kbps；
- 开启游戏加速功能，为游戏数据预留专用通道；
- 设置连接数限制条目，限制每台主机的最大连接数为 250 条；
- 设置端口 5 为监控端口，端口 3 为被监控端口。端口 5 连接到装有公安局监控软件的电脑上。（如果中心交换机支持端口镜像功能，建议在中心交换机上做监控）

5.3 典型组网拓扑

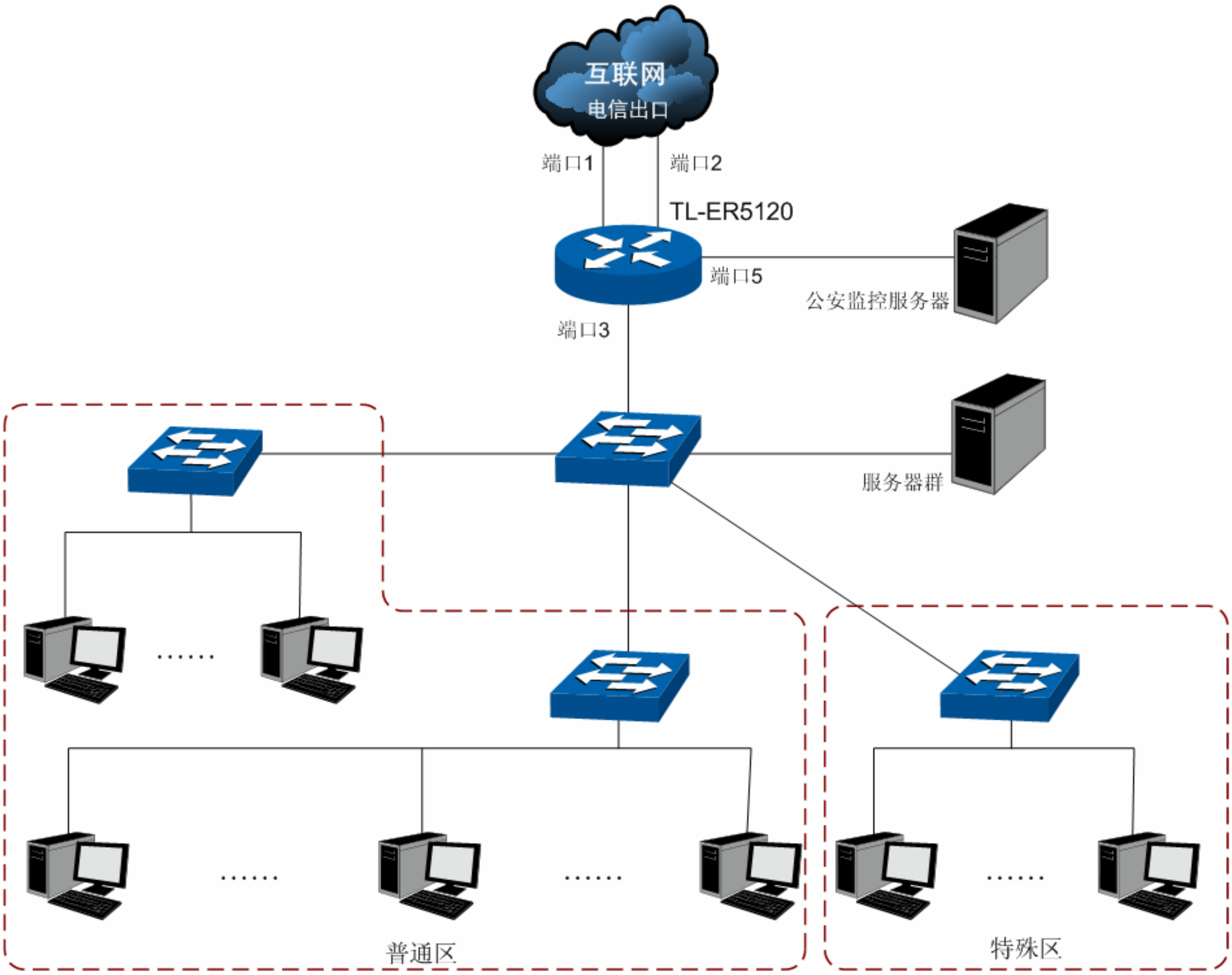


图 5-1 网吧典型应用组网拓扑

5.4 典型配置步骤

可以通过连接到路由器 LAN 口的计算机对路由器进行配置。

计算机的 IP 地址可以自动获取，也可以手动设置。手动设置时请确保计算机 IP 地址与路由器 LAN 口在同一网段（默认路由器 LAN 口处于为 192.168.1.0/24 网段），然后在 Web 浏览器的地址栏中输入“http://192.168.1.1”（如果您已修改路由器 LAN 口 IP 地址，请输入新地址），按下回车键后出现登录窗口，在登录窗口中输入用户名：admin，密码：admin（如果您已修改密码，请输入新密码），点击<登录>按钮即可进入路由器 Web 配置界面。

5.4.1 系统模式设置

设置系统模式为 NAT 模式。设置界面进入方法：**系统模式 >> 系统模式**。选择“NAT 模式”后点击<保存>按钮。

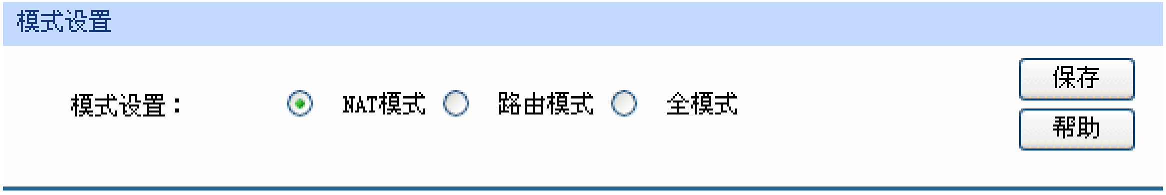


图 5-2 系统模式设置

5.4.2 WAN模式设置

设置路由器为双 WAN 口模式。设置界面进入方法：**接口设置 >> WAN 模式 >> WAN 模式**。选择"双 WAN 口"模式后点击<保存>按钮，此时接口 1 和接口 2 成为路由器的两个 WAN 口。

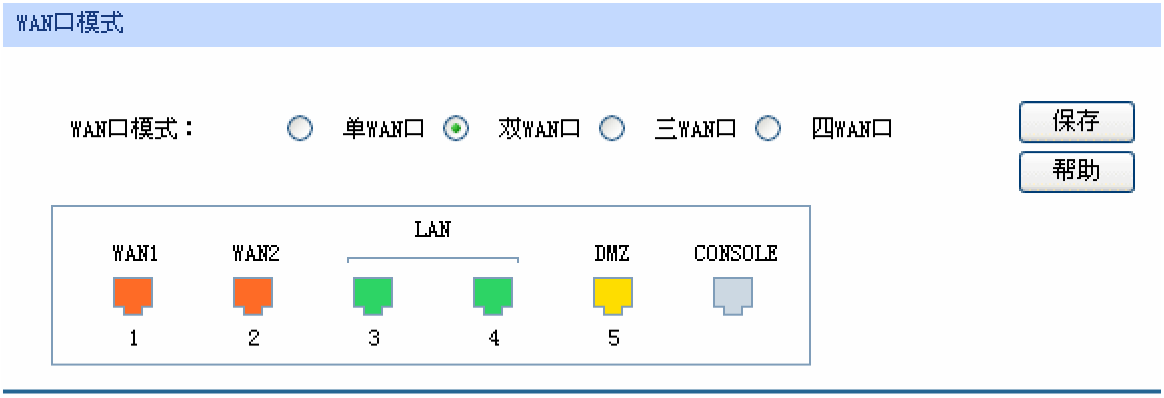


图 5-3 系统模式设置

5.4.3 上网方式设置

设置两个WAN口的连接方式为静态IP。设置界面进入方法：**接口设置 >> WAN设置 >> WAN1 设置**。选择"静态IP"，填入电信提供的IP地址、子网掩码、网关地址等信息，设置上下行带宽均为10000Kbps，如图 5-4。点击<保存>按钮即可，WAN2 口的设置方法相同。



图 5-4 WAN 口设置静态 IP 连接方式

5.4.4 局域网主机IP设置

为了能将网吧内所有主机的 IP 与 MAC 绑定、防止 IP 参数被他人随意修改，建议禁用 DHCP 功能，为每台主机手动分配 IP 参数，分配时可以将 IP 地址号与座位编号对应起来，方便网络管理和维护。例如，座位编号 100，其主机对应 IP 地址分配为 192.168.1.100。

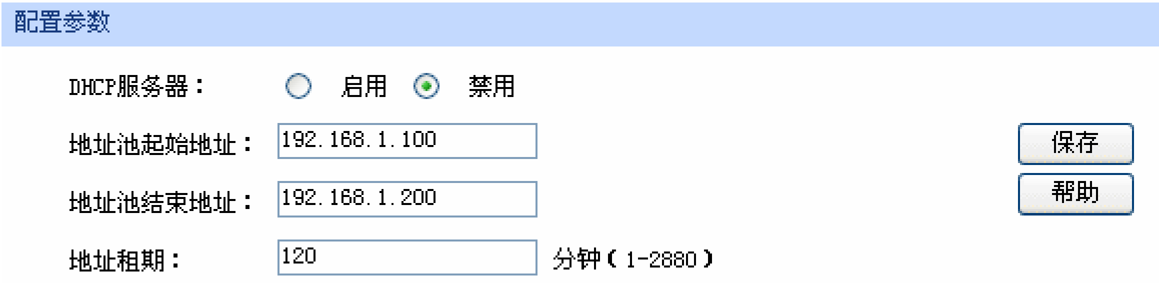


图 5-5 禁用 LAN 口的 DHCP 功能

5.4.5 局域网ARP攻击防护设置

可以采用 ARP 扫描和手动设置两种方式绑定 IP 与 MAC 信息。首次设置时，请先使用扫描方式绑定大部分的 ARP 信息，如果还有个别特殊条目，还可以通过手动设置绑定。

1. 扫描并将条目导入 ARP 绑定列表

指定范围进行ARP动态扫描。设置界面进入方法：**安全策略 >> ARP防护 >> ARP扫描**。进行ARP扫描的前提是当前局域网内不存在ARP攻击。设置如图 5-6。

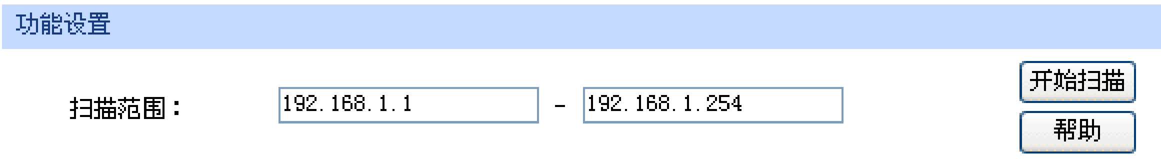


图 5-6 设置 ARP 扫描的地址范围

开启网吧中需要进行ARP绑定的所有主机，点击<开始扫描>按钮，得到扫描结果如图 5-7。



扫描结果

选择	序号	IP地址	MAC地址	状态
☐	1	192.168.1.2	00-19-66-64-ED-33	---
☐	2	192.168.1.5	00-19-66-35-E6-D4	---
☐	3	192.168.1.115	00-19-66-5C-4B-1E	---
☐	4	192.168.1.150	00-19-66-33-8E-4B	---
☐	5	192.168.1.155	00-19-66-35-E1-5C	---

图 5-7 ARP 扫描结果列表

选中需绑定的ARP条目，或点击<全选>按钮，再点击<导入>按钮即完成ARP绑定。ARP绑定列表如图 5-8。界面进入方法：**安全策略 >> ARP防护 >> IP MAC绑定**。



绑定列表

选择	序号	IP地址	MAC地址	状态	备注	设置
☐	1	192.168.1.2	00-19-66-64-ED-33	已生效	---	
☐	2	192.168.1.5	00-19-66-35-E6-D4	已生效	---	
☐	3	192.168.1.115	00-19-66-5C-4B-1E	已生效	---	
☐	4	192.168.1.150	00-19-66-33-8E-4B	已生效	---	
☐	5	192.168.1.155	00-19-66-35-E1-5C	已生效	---	

全选 生效 不生效 删除 搜索

图 5-8 导入后生效的 ARP 绑定列表

2. 手动设置 ARP 绑定条目

手动设置IP与MAC绑定信息并新增至ARP绑定列表。设置界面进入方法：**安全策略 >> ARP防护 >> ARP绑定 >> IP MAC绑定**。假设现在需要添加座位号为 200 的主机IP MAC信息，该主机MAC地址为00-11-22-33-44-aa，则填入相应的IP、MAC地址，备注处标明“200 座”，如图 5-9。选择“生效”后点击<新增>按钮，则条目绑定成功。其他待绑定的条目也可依次手动添加。

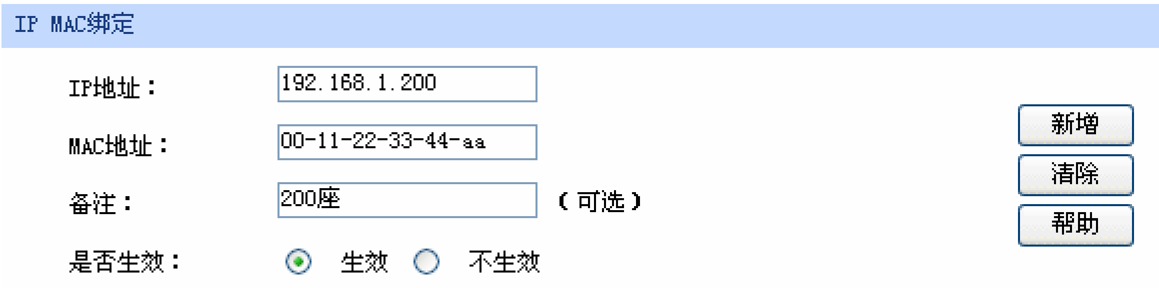


图 5-9 手动设置 200 号座位主机的 IP MAC 信息

3. 设置 ARP 防欺骗功能

进入IP MAC绑定界面，进入方法：**安全策略 >> ARP防护 >> IP MAC绑定**。在“功能设置”处勾选所有条目，并将路由自动发送GARP包的发包间隔设置为 1ms，如图 5-10。点击<保存>按钮即启用ARP防欺骗功能。

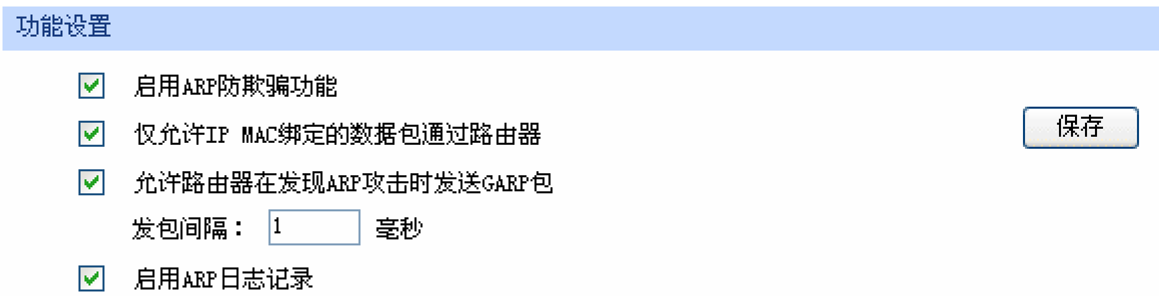


图 5-10 开启 ARP 防欺骗功能

5.4.6　　广域网ARP攻击防护设置

可通过绑定 WAN 口网关及 MAC 地址来进行广域网 ARP 攻击防护。

首先，需要通过ARP扫描获取网关MAC地址，设置界面进入方法：**安全策略 >> ARP防护 >> ARP扫描**。在扫描范围填入WAN口网关IP地址 58.51.128.254，点击<开始扫描>按钮，如图 5-11。扫描结束后，在扫描结果中，就能看到网关对应的MAC地址。

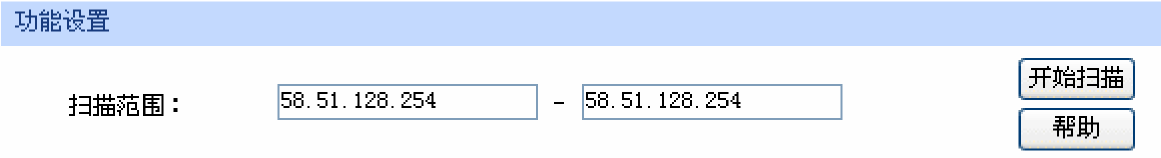


图 5-11 设置动态扫描 ARP 的地址范围为 WAN 口网关 IP

在扫描结果列表中获得 WAN 口网关 MAC 地址后，勾选此条目，点击<导入>按钮，完成绑定操作。

5.4.7　　网络攻击防护设置

设置界面进入方法：**安全策略 >> 攻击防护 >> 攻击防护**。勾选所需开启的攻击防护选项，如图 5-12。点击<保存>按钮即可。

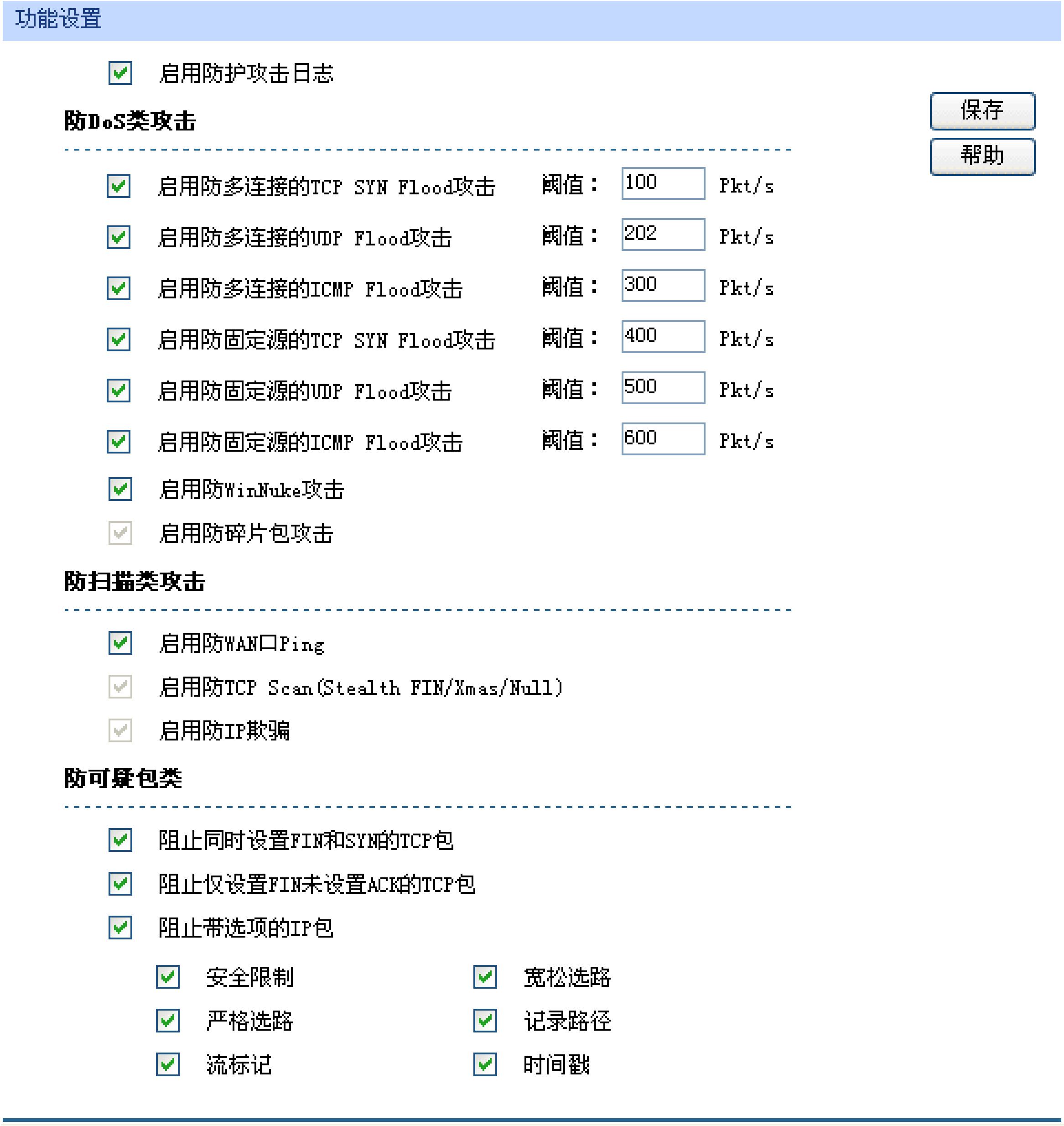


图 5-12 启用网络攻击防护功能

5.4.8 带宽控制设置

带宽控制需要通过设置接口总带宽和具体的带宽控制规则来实现。

1. 接口总带宽设置

设置界面进入方法：**传输控制 >> 带宽控制 >> 综合设置**。勾选“启用普通带宽控制”，WAN1 口和WAN2 口的出口与入口带宽均为 10000Kbps。如图 5-13。点击<保存>按钮即可。



图 5-13 启用带宽控制

2. 带宽控制规则设置

假设现已手动设置网吧普通区主机 IP 地址范围：192.168.1.2 - 192.168.1.101，特殊区主机 IP 地址范围：192.168.1.102 - 192.168.1.151，您可以通过以下步骤设置带宽控制规则。设置界面进入方法：**传输控制 >> 带宽控制 >> 带宽控制规则**。

首先为普通区IP地址为 192.168.1.2 - 192.168.1.101 的主机设置带宽控制规则。选择数据流量为 LAN -> WAN-ALL，带宽模式为独立，上行与下行最小保证带宽各为 100Kbps，最大限制带宽各为 800Kbps，其余项目保持默认设置，选择启用，如图 5-14。点击<新增>按钮，则普通区所有主机带宽控制设置成功。



图 5-14 设置普通区主机的带宽控制规则

参考普通区的设置方法为特殊区IP地址为 192.168.1.102 - 192.168.1.151 的主机设置带宽控制规则。选择数据流向为LAN -> WAN-ALL，带宽模式为独立，上行与下行最小保证带宽各为 100Kbps，最大限制带宽各为 1000Kbps，其余项目保持默认设置，选择启用，如图 5-15。点击<新增>按钮，则单机带宽控制设置成功。



图 5-15 设置特殊区主机的带宽控制规则

5.4.9　游戏加速设置

设置界面进入方法：**传输控制 >> 带宽控制 >> 游戏加速**。勾选“启用游戏加速”，保证带宽大小为 25%，如图 5-16。点击<保存>按钮即完成游戏加速设置。

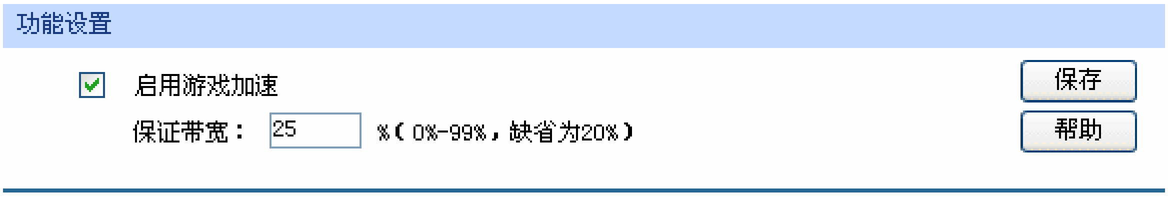


图 5-16 启用游戏加速功能

5.4.10　连接数限制设置

设置界面进入方法：**传输控制 >> 连接数限制 >> 连接数限制规则**。设置 192.168.1.2 - 192.168.1.151 范围内的IP地址发起的最大连接数为 250，勾选启用，如图 5-17。点击<新增>按钮完成设置。

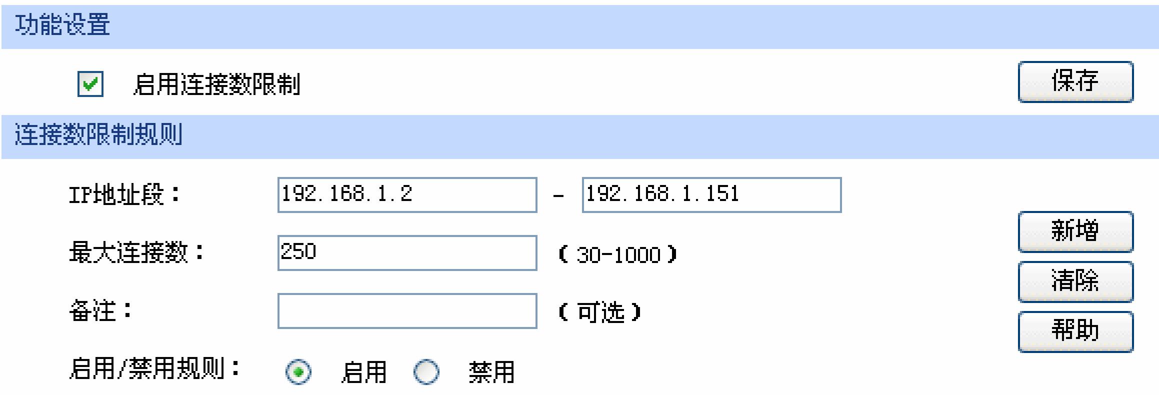


图 5-17 启用连接数限制功能

5.4.11 端口监控设置

设置界面进入方法：**端口设置 >> 端口监控**。勾选“启用端口监控”，监控模式为输入输出监控，监控端口选择端口 5，被监控端口选择端口 3，如图 5-18。点击<保存>按钮即完成端口监控设置。



图 5-18 设置端口监控功能

以上所有步骤设置完成后，网吧就可以按规划正常运营了。

第6章 命令行简介

CLI(Command Line Interface，命令行接口）即命令行，TL-ER5120 路由器提供了一个用于 CLI 配置的 Console 口。可以通过控制台（比如超级终端）和在局域网内通过 Telnet 进入命令行界面进行设置。

以下介绍通过超级终端访问 CLI 的具体步骤和一些常用的 CLI 命令。

6.1 搭建平台

首先，使用 Console 线连接路由器和计算机的 Console 口。

选择 开始>所有程序>附件>通讯>超级终端，打开超级终端。



图 6-1 打开超级终端

弹出如图 6-2所示的连接描述窗口，在名称处键入一个名称，点击<确定>。



图 6-2 连接描述窗口

在图 6-3中选择连接串口（单串口默认COM1 口），点击<确定>。

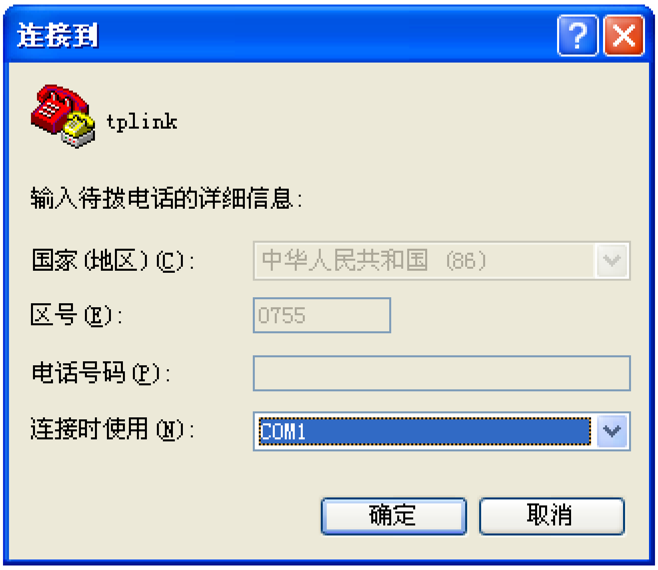


图 6-3 连接参数窗口

在图 6-4中对端口进行参数设置，每秒位数 115200，数据位 8，奇偶校验无，停止位 1，数据流控制无，点击<确定>。

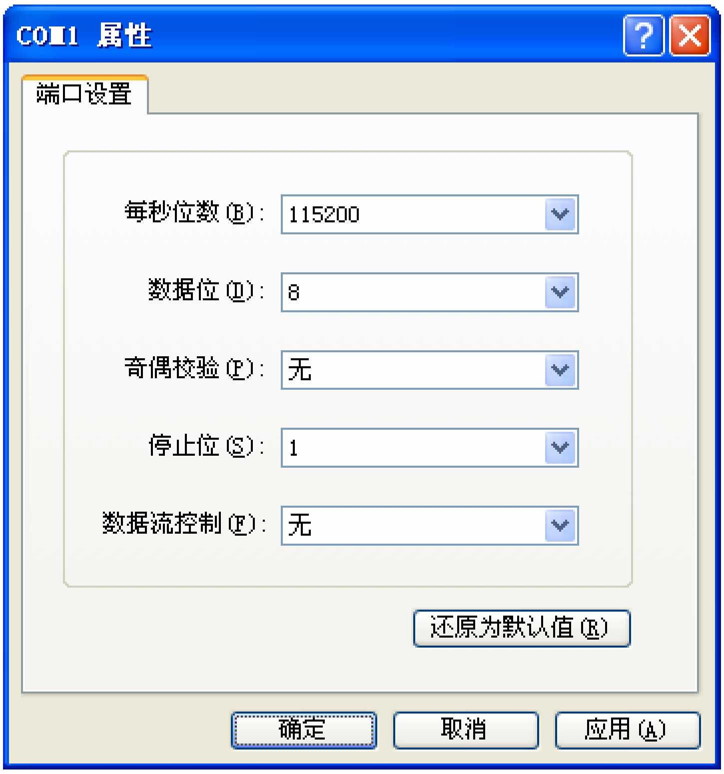


图 6-4 端口属性设置

在图 6-6超级终端主窗口选择 文件>属性>设置，在图 6-5中选择终端仿真类型为VT100 或自动检测，点击<确定>。



图 6-5 连接属性设置

在超级终端主窗口中按下回车键，就可以看到“TP-LINK>” 的提示符了。如图 6-6所示。

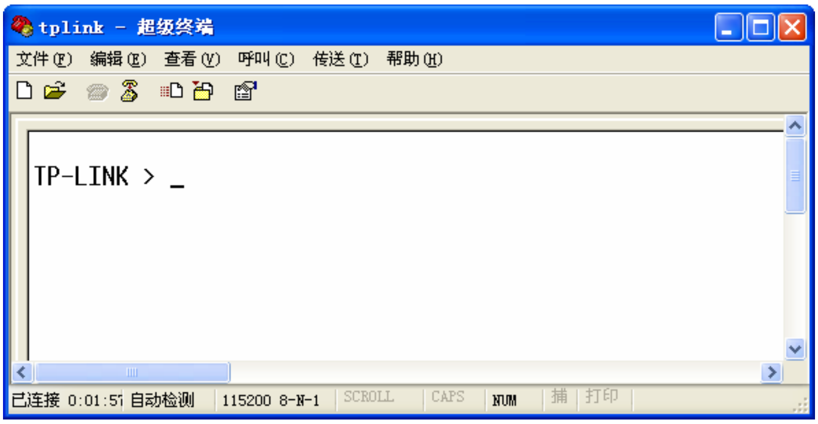


图 6-6 命令行主窗口

6.2 界面模式

TL-ER5120 的 CLI 提供了两个界面模式：用户模式和特权模式。用户模式下只具有基本的权限，比如查看系统的信息等。特权模式下则拥有管理路由器的权限，可以进行各种配置操作等。这样就可以对不同的用户进行适当的权限管理。

用户模式：Telnet 登录时，需输入路由器的用户名和密码，默认为 admin/admin，Console 连接登录时不需要密码。登录后，用户处于用户模式下，拥有的权限为参观级。可以进行简单的查询操作，不能修改路由器的各种配置信息。

特权模式：用户在用户模式下进行密码验证，验证通过就可以进入特权模式。拥有管理级的权限，可以对路由器进行各种配置操作。

默认情况下，CLI 用户处于用户模式下。用户可以自由的在用户模式和特权模式之间进行切换，方式如下：

模式	访问方法	提示符	离开或访问下一模式
用户模式	与路由器建立连接即进入该模式。	TP-LINK >	输入 exit 命令断开与路由器的连接（Console 连接时无法断开） 要进入特权模式，输入 enable 命令。
特权模式	在用户模式下，使用 enable 命令进入该模式，初始密码 admin。	TP-LINK #	输入 exit 命令断开与路由器连接（Console 连接时无法断开） 要返回到用户模式，输入 disable 命令。

如图 6-7所示：

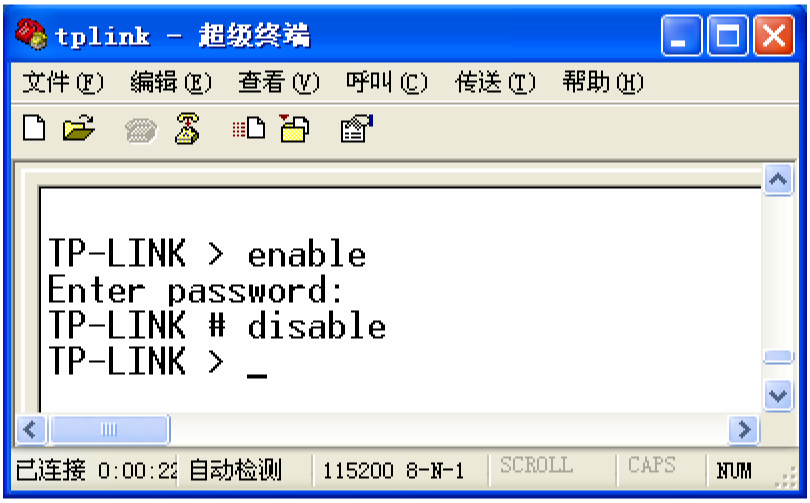


图 6-7 用户模式与特权模式切换

6.3 在线帮助

TL-ER5120 提供了命令行在线帮助：

1) 在任一模式下，键入“?”获取该视图下所有的命令及其简单描述。

```
TP-LINK > ←键入“?”键
disable          - Exit the privileged mode
enable           - Enter the privileged mode
exit             - Exit the CLI (only for telnet)
history          - Show command history
ip               - Display or Set the IP configuration
ip-mac           - Display or Set the IP mac bind configuration
sys              - System manager
user             - User configuration
```

2) 键入一命令，后接以空格分隔的“?”，如果该命令行位置有关键字，则列出全部关键字及其简单描述。例如：

```
TP-LINK > ip ←按下“空格”“?”键
get              - Get the ip configuration
```

3) 键入一字符串，其后紧接“?”，列出以该字符串开头的所有命令。例如：

```
TP-LINK > dis←按下“?”键
disable
```

4) 键入命令的某个关键字的前几个字母，按下<Tab>键，如果以输入字母开头的关键字唯一，则可以显示出完整的关键字。例如：

```
TP-LINK > dis←按下“Tab”键
disable
```

5) 命令的输入完成之后，后接以空格分隔的“?”，会显示出一个回车符，表示此时可以执行该命令。例如：

```
TP-LINK # enable ←按下“空格”“?”键
<cr>
```

6.4 命令介绍

TL-ER5120 提供了一些 CLI 命令，通过这些命令可以管理路由器和用户信息。为便于您理解，每条命令后面会注释该条命令的含义。

6.4.1 接口设置

ip 命令。可以使用该命令查看或设置当前系统中相关接口的 IP 地址和子网掩码，查看命令可以在用户模式和特权模式下使用，设置功能只能在特权模式下使用。

```
TP-LINK > ip get lan
Lan Ip:    192.168.1.1
Lan Mask:  255.255.255.0
```

获取 LAN 口配置信息的命令。

```
TP-LINK # ip set lan address 192.168.1.20
```

设置路由器 LAN 口 IP 地址为 192.168.1.20。如果返回 Operation succeeded!表示操作成功，如发生错误会有提示。

```
TP-LINK # ip set lan mask 255.255.0.0
```

设置路由器 LAN 口子网掩码为 255.255.0.0。

6.4.2 IP MAC 绑定设置

ip-mac 命令。可以使用该命令查看或设置当前系统中 IP MAC 绑定的模式。设置功能只能在特权模式下使用，查看命令可以在用户模式和特权模式下使用。IP MAC 绑定的模式有两种：普通绑定模式(normal)和强制绑定模式(restrict)。

```
TP-LINK > ip-mac get mode
Ip-mac Bind Mode:  normal
```

获取当前 IP MAC 绑定模式。

```
TP-LINK # ip-mac set mode restrict
```

设置当前 IP MAC 绑定模式为强制绑定模式。

6.4.3 系统管理

sys 命令。可以使用该命令进行相关的系统管理操作，包括配置文件的导入导出、恢复出厂配置、重启系统和升级软件等。

```
TP-LINK # sys reboot
This command will reboot system, Continue?[Y/N]
```

重启系统。Y 即 YES，表确认；N 即 NO，表取消。

```
TP-LINK # sys restore
This command will restore system, Continue?[Y/N]
```

恢复出厂配置。Y 即 YES，表确认；N 即 NO，表取消。

```
TP-LINK # sys export config
Server address: [192.168.1.101]192.168.1.100
Username: [admin]ftp
Password: [admin]ftp
File name: [config.bin]
Try to save the configuration file < config.bin > ...
Save configuration file < config bin > succeed, file size is 7104 bytes.
```

配置文件导出。

举例：现有一台 IP 地址为 192.168.1.100 的 FTP 服务器，服务的用户名/密码是 ftp/ftp，如需将当前配置文件以默认文件名 config.bin 保存到该 FTP 服务器上，设置如左。

说明

- 配置文件的导出、导入、系统升级都需要使用 FTP 服务。在需设置的参数中，Server address 是提供 FTP 服务的主机 IP 地址，Username/Password 是该 FTP 服务的登录名/密码，File name 是配置文件名（如果已存在同名的配置文件，请更改文件名）。
- 中括号内是默认设置，可在其后输入实际参数，如果无需改动直接回车确认即可。
- TL-ER5120 默认连接到使用 21 端口的 FTP 服务器。
- 由于导出、导入、系统升级等功能需要在 FTP 服务器上进行读写操作，因此特别需要注意您指定的帐号必须具有相应权限。

```
TP-LINK # sys import config
Server address: [192.168.1.101]
Username: [admin]
Password: [admin]
File name: [config.bin]
Try to get the configuration file < config.bin > ...
Get configuration file < config bin > succeed, file size is 7104 bytes.
```

配置文件导入。说明同上。

```
TP-LINK > sys show
CPU Used Rate:    1%
```

查看系统信息。该命令将会显示当前系统的 CPU 利用率。

```
TP-LINK # sys update
Server address: [192.168.1.101]
Username: [admin]
Password: [admin]
File name: [update.bin]
Try to get the update file < update.bin > ...
Get update file < update bin > succeed, file size is 2298608 bytes.
```

系统软件升级。

6.4.4 用户信息管理

user 命令。可以使用该命令查询或修改登录 CLI 的用户名和密码。在用户模式下，可以修改参观级用户的密码，由于参观级用户和管理员用户共用一个用户名，因此在用户模式下不能修改用户名；在特权模式下可以修改管理员级用户的用户名和密码。

```
TP-LINK > user get
Username: admin
Password: admin
```

查询当前参观级用户的用户名及密码。

`TP-LINK > ` **`user set password`**
`Enter old password:`
`Enter new password:`
`Confirm new password:`
	修改参观级用户的密码。

`TP-LINK # ` **`user get`**
`Username: admin`
`Password: admin`
	查询当前管理员级用户的用户名及密码。

`TP-LINK # ` **`user set password`**
`Enter old password:`
`Enter new password:`
`Confirm new password:`
	修改管理员级用户的密码。

`TP-LINK # ` **`user set username`** `Enter new username: tplink`	修改管理员级用户的用户名。

注意：

用户名和密码长度为 1-31 个字符，用户名和密码只能使用字母和数字，且区分大小写。

6.4.5 历史命令管理

history 命令。可以使用该命令查看或清除系统中的历史命令。

`TP-LINK > ` **`history`**
`1. history`
`2. sys show`
`3. history`
	查看历史命令。

```
TP-LINK > history clear
1. history
2. sys show
3. history
4. history clear
```

清除历史命令。

6.4.6 退出CLI

exit 命令。可以使用该命令退出系统。但仅限于 Telnet 环境，Console 环境下不会退出。

```
TP-LINK > exit
```

退出系统。

附录A 常见问题

问题 1：无法登录路由器 Web 管理界面该如何处理？

1. 如果您是第一次使用此路由器，请参考以下步骤：

    1) 确认网线已正常连接到了路由器的 LAN 口，对应的指示灯闪烁或者常亮。

    2) 访问设置界面前，建议您将计算机设置成“自动获取 IP 地址”，由开启 DHCP 服务的路由器自动给计算机分配 IP 地址。如果需要给计算机指定静态 IP 地址，请将计算机的 IP 与路由器 LAN 口 IP 设置在一网段，路由器默认 LAN 口 IP 地址为：192.168.1.1，子网掩码：255.255.255.0，计算机的IP地址应设置为：192.168.1.X（X为2至254之间任意整数)，子网掩码为：255.255.255.0。

    3) 使用 ping 命令检测计算机与 TL-ER5120 之间的连通性。

    4) 若上述提示仍不能帮助您登录到路由器管理界面，请您将路由器恢复为出厂配置。

2. 如果您修改过路由器的管理端口，则注意下次登录时您需要以“http://管理 IP:XX”的方式登录，XX 为修改后的端口号，如 **http://192.168.1.1:8080**。

3. 如果您之前可以正常登录，现在不能登录，则有可能是他人修改了路由器的配置导致的（尤其在开启了远程 Web 管理的情况下），建议恢复出厂配置，修改路由器的管理端口、修改用户名和密码，做好保密措施。

4. 如果恢复出厂配置后仍然无法登录或开始一段时间能登录，但过一段时间后又不能登录，则可能是遭受了 ARP 欺骗，建议查找欺骗源、查杀病毒或将其隔离。

5. 请您检查是否设置了 IE 代理，如果设置了 IE 代理，请先将代理取消。

问题 2：忘记路由器用户名和密码怎么办？如何恢复出厂配置？

忘记用户名密码时可以将 TL-ER5120 通过 Reset 键恢复至出厂配置。需要注意的是：恢复出厂配置时路由器原有配置信息将丢失。

恢复出厂配置操作方法：在路由器通电的情况下，使用尖状物按住路由器前面板的 Reset 键，等待 3-5 秒后，见到 M1 灯长亮 2-5 秒，松开按键，待 M1 和 M2 两灯同时快闪约 1 秒，此时您已成功恢复出厂配置。路由器出厂默认管理地址是 **http://192.168.1.1**，默认用户名/密码是 admin/admin。

问题 3：忘记路由器管理端口怎么办？

可尝试使用第三方端口扫描工具，扫描路由器 LAN 口开放的 TCP 端口，根据扫描出的端口依次尝试登录。如果通过这种方法没有达到预期效果，那么只能将路由器恢复为出厂配置。

问题 4：为什么开启了远端管理后，非局域网段不能登录管理路由器？

1. 非局域网段要登录路由器的 IP 地址是否是被允许远端访问路由器的。

2. 路由器的管理端口是否已经修改过，如果修改过，则应以“http://WAN 口 IP:XX”的方式登录，XX 为修改后的管理端口，如 **http://202.160.58.67:8080**。

3. 路由器的管理端口是否已经在虚拟服务器中被映射为局域网主机的某个服务端口，如果已经被映射为主机的服务端口，则应更改主机服务的端口或更改路由器的管理端口为其它端口。

4. 路由器虚拟服务器的 NAT DMZ 服务是否启用，如需远程管理路由器，请禁用 NAT DMZ 服务。

问题 5：路由器某些功能设置需要填写子网掩码值划分地址范围，一般子网掩码都有哪些值？

子网掩码是一个 32 位的二进制地址，以此来区别网络地址和主机地址。子网划分时，子网掩码不同，所得到的子网不同，每个子网能容纳的主机数目不同。

常用的子网掩码值有 **8**（即 A 类网络的缺省子网掩码 255.0.0.0）、**16**（即 B 类网络的缺省子网掩码 255.255.0.0）、**24**（即 C 类网络的缺省子网掩码 255.255.255.0）、**32**（即单个 IP 地址的缺省子网掩码 255.255.255.255）。

附录B 术语表

	英文术语	中文名称	定义或描述
A	ADSL(Asymmetrical Digital Subscriber Line)	非对称数字用户线路	非对称数字用户线路，是一种宽带接入技术，是目前应用最广的宽带接入方式。它利用双绞铜线向用户提供两个方向上速率不对称的宽带信息业务。
	ALG(Application Layer Gateway)	应用层网关	工作在应用层的网关，通过处理应用层的数据使穿透网关进行的网络应用能够正常工作。
	ARP(Address Resolution Protocol)	地址解析协议	一种把 IP 地址转换成物理地址的协议。
D	DDNS(Dynamic Domain Name Server)	动态域名解析服务器	实现将固定域名解析为动态变化的 IP 地址的域名解析服务器。
	DHCP(Dynamic Host Configuration Protocol)	动态主机配置协议	为网络中的主机动态分配 IP 地址、子网掩码、网关、DNS 等信息。
	DMZ(Demilitarized Zone)	非军事区	路由器对此区域主机不进行保护，广域网主机可主动访问这些主机。
	DNS(Domain Name Server)	域名解析服务器	实现将域名解析为 IP 地址的域名解析服务器。
F	Flood	洪泛	是攻击程序大量快速模仿某种连接请求，导致 CPU 繁忙或网络瘫痪。
	FTP(File Transfer Protocol)	文件传输协议	在基于 TCP/IP 网络和互联网的联网计算机之间传送文件的标准协议。
G	GMT(Greenwich Mean Time)	格林威治标准时间	以经过格林威治的本初子午线为标准的国际统一时间。
	GARP(gratuitous ARP)	免费地址解析协议	主机通过 GARP 向广播域发送不期望回复的 ARP 包以广播自己的 IP 对应的 MAC 地址，或者检测以太网内是否有 IP 冲突。
H	H.323	-	H.323 为现有的分组网络 PBN（如 IP 网络）提供多媒体通信标准。它规定了不同的音频、视频或数据终端协同工作所需的操作模式。
	HTTP(Hypertext Transfer Protocol)	超文本传输协议	常用于 WWW 服务器与客户端之间传输文件。

	英文术语	中文名称	定义或描述
I	ICMP(Internet Control Messages Protocol)	网间控制报文协议	ICMP 传递差错报文以及其他需要注意的信息。ICMP 报文通常被 IP 层或更高层协议（TCP 或 UDP）使用。
	Internet	因特网/国际互联网/网际网	是使用公用语言互相通信的，许多路由器和公共互联网连接而成的全球网络。
	IP(Internet Protocol)	网际协议/互联网协议	IP 是 TCP/IP 协议族中最为核心的协议。所有的 TCP、UDP、ICMP 及 IGMP 数据都以 IP 数据报格式传输。
	ISP(Internet Service Provider)	互联网服务提供商	提供因特网接入服务的提供商。
L	LAN(Local Area Network)	局域网/本地网	指将位于相对有限区域内的一组计算机、打印机和其他设备连接起来的通讯网络。LAN 内部连接的设备都能与其中的其他设备交互。
M	MAC address(Media Access Control address)	介质访问控制地址	MAC 协议主要负责控制与连接物理层的物理介质，协议中定义的 MAC 地址是由厂商指定的用来标识网络节点的全球唯一的硬件地址。由 6 组编码组成，每组编码表示为 2 个 16 进制数。
	MTU(Maximum Transmission Unit)	最大传输单元	网络中传输数据包的最大长度。
N	NAT(Network Address Translator)	网络地址转换	将局域网的 IP 地址转换成用于互联网的外部 IP 地址。
	NAT DMZ/pseudo DMZ(NAT Demilitarized Zone)	非军事区域/隔离区	是在 NAT 网关应用上的一种特殊服务。开启 NAT DMZ 服务后，网关会将所有广域网发起的、不符合所有现有连接和转发规则的数据全部转发向您设置的 NAT DMZ 主机地址。
	NTP Server	网络时间服务器	用于互联网上的计算机时间同步。
P	POP3(Post Office Protocol 3)	邮局协议第 3 版本	规定了将个人计算机连接到互联网的邮件服务器和下载电子邮件的方法的一种协议。
	Port VLAN	基于端口的 VLAN	基于同一路由器端口划分的 VLAN，即不可以跨越路由器划分 VLAN。
	PPPoE(Point-to-Point Protocol over Ethernet)	点对点以太网承载协议	点对点以太网承载协议在以太网上承载 PPP 协议封装的报文，它是目前使用较多的业务形式。
	Private	私有的	用于表示网络是局域网（私有网络）。
	Public	共有的，公共的	用于表示网络是广域网（公有网络）。

	英文术语	中文名称	定义或描述
S	SMTP(Simple Mail Transfer Protocol)	简单邮件传输协议	用于电子邮件的传输。
	SSH(Secure Shell Protocol)	安全外壳协议	SSH 是一种在不安全网络上提供安全远程登录及其它安全网络服务的协议。
T	TCP-ACK(ACKnowledgment)	确认	TCP 首部中的确认标志。
	TCP-FIN(Finish)	结束	TCP 首部中的结束标志。
	TCP-SYN(SYNchronous)	同步	TCP 首部中的同步序号标志。
	TCP(Transfer Control Protocol)	传输控制协议	传输控制协议是一种面向连接的、可靠的传输层协议。
	TCP/IP(Transmission Control Protocol/ Internet Protocol)	传输控制协议和互连网协议	用于网络的一组通讯协议，IP 提供无连接的数据报传输机制，TCP 提供一种面向连接的、可靠的字节流服务。
	Telnet(Telecommunication Network protocol)	远程终端协议	是在 TCP/IP 网络上，标准的提供远程登录功能的应用。
U	UDP(User Datagram Protocol)	用户数据报协议	面向无连接的、不可靠的传输层协议。
	UPnP(Universal Plug and Play)	通用即插即用	通用即插即用是一种用于 PC 机和智能设备（或仪器）的常见对等网络连接的体系结构。
	URL (Uniform Resource Locator)	统一资源定位符	互联网上的资源地址。
V	VLAN(Virtual Local Area Network)	虚拟局域网	组成局域网的逻辑子组。一个 VLAN 是一个按功能、组、或者应用被逻辑分段的交换网络，并不考虑使用者的物理位置。一个端口上接受到的包被发往属于同一个 VLAN 的接收端口，不同 VLAN 的网络设备无法通讯。
W	WAN(Wide Area Network)	广域网	在很宽的地理区域内为用户服务的数据通信网络，此网络通常使用由公共设备商提供的传输设备。

附录C 规格参数

参数项		参数内容
支持的标准和协议		IEEE 802.3、IEEE 802.3u、IEEE 802.3x、TCP/ IP、DHCP、ICMP、NAT、PPPoE、SNTP、HTTP、DNS
端口	LAN 口	至少 1 个至多 4 个 10/100M 自适应 RJ45 端口(Auto MDI/MDIX)
	WAN 口	至少 1 个至多 4 个 10/100M 自适应 RJ45 端口(Auto MDI/MDIX)
	DMZ 口	至多 1 个 10/100M 自适应 RJ45 端口(Auto MDI/MDIX)
	其它	1 个 Console 端口
网络介质		10BASE-T：3 类或 3 类以上非屏蔽双绞线(UTP)(≤100m)
		100BASE-TX：5 类非屏蔽双绞线(UTP)(≤100m)
LED 指示	LAN/WAN 口	Link/Act 指示灯、100M 速率指示灯
	其它	PWR 电源指示灯、M1/M2 系统状态指示灯、DMZ 接口状态指示灯
外形尺寸 (L x W x H)		440mm x 220mm x 44mm
散热方式		自然散热
电源及功耗		输入：100-240V~ 50/60Hz 0.6A
		功耗：最大 9.3W
使用环境		工作温度：0ºC ~ 40ºC
		存储温度：-40ºC ~ 70ºC
		工作湿度：10% ~ 90%RH 不凝结
		存储湿度：5% ~ 90%RH 不凝结

深圳市普联技术有限公司
TP-LINK TECHNOLOGIES CO., LTD.
技术支持热线：400-8863-400
公司地址：深圳市南山区桃源街道平山大园工业区南区2栋1-6楼
技术支持E-mail：smb@tp-link.com.cn
http://www.tp-link.com.cn